Topic 4
Topic 2
Topic 3
Topic 1
Topic 5

Topic1
p70

Topic2
p101-102, p104-105, p115, p147, p158-159, p187

Topic3
p89-93, p96-101, p105, p109-110, p112-114, p116-119, p121-122, p124-129, p131, p133-134, p136, p139, p141-147, p150-151, p153-154, p157, p159-162, p164-168, p171-176, p183, p185-195

Topic4
p100, p191

Topic5
p89-90, p92, p94, p96-99, p107-111, p113, p115-116, p119, p129-130, p136-137,

Luxembourg, le 24 juillet 2017

À adapter aux entreprises et entités surveillées par la CSSF

CIRCULAIRE CSSF 17/661

Concerne: Adoption des orientations conjointes émises par les trois autorités européennes de surveillance (EBA/ESMA/EIOPA) sur les facteurs de risque de blanchiment de capitaux et de financement du terrorisme

Mesdames, Messieurs,

L'objet de la présente circulaire est de porter à votre attention l'adoption par les trois autorités européennes de surveillance (EBA, ESMA, EIOPA) des Orientations conjointes sur les obligations de vigilance simplifiée et renforcée et les facteurs que les établissements de crédit et les établissements financiers (« les professionnels ») doivent prendre en compte lors de l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme en rapport avec des relations d'affaires ou des transactions occasionnelles (« Les Orientations ») sur base des articles 17 et 18, paragraphe 4, de la Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission[1].

Les Orientations entreront en vigueur le **26 juin 2018**.

Les Orientations ont pour objectif de fournir des lignes directrices sur les différents facteurs de risques de blanchiment de capitaux et de financement du terrorisme que les professionnels doivent prendre en compte dans le cadre de leur évaluation des risques. Par ailleurs, les Orientations précisent aussi comment les professionnels peuvent ajuster les mesures de vigilance en matière de lutte contre le blanchiment de capitaux et de financement du terrorisme (« LBC/FT ») en fonction du niveau de risque présent dans une relation d'affaires ou dans une transaction occasionnelle. Ainsi, elles comportent des exemples de mesures de vigilance, soit simplifiées en cas de risque plus faible, soit renforcées afin d'atténuer des risques identifiés plus élevés.

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015L0849&from=FR

Dans une première partie (Titre II) sont fournies des informations d'application générale en matière d'obligations de vigilance. Des informations plus spécifiques renseignant sur les facteurs de risques présents dans certains secteurs déterminés et les mesures de vigilance y relatives, sont fournies dans une deuxième partie (Titre III). Les sujets abordés dans cette deuxième partie sont les suivants :

- Relations de correspondance bancaire ;
- Banques de détail ;
- Emetteurs de monnaie électronique ;
- Etablissements de paiement de transmission de fonds (« money remitters ») ;
- Gestion de patrimoine (« wealth management ») ;
- Prestataires de financement commercial (« trade finance ») ;
- Entreprises d'assurance-vie ;
- Entreprises d'investissement ;
- Prestataires de fonds d'investissement.

Il convient de souligner que ni les facteurs de risques, ni les mesures de vigilance décrits dans les Orientations ne sont à considérer comme exhaustifs.

Sur base des Orientations les professionnels devraient pouvoir prendre des décisions éclairées en fonction des risques BC/FT pour gérer efficacement leurs relations d'affaires et les transactions occasionnelles, tout en tenant compte des attentes des autorités de surveillance européennes quant à la manière de s'acquitter d'importantes obligations de LBC/FT.

Il convient de souligner en plus que les Orientations peuvent être actualisées et complétées selon les besoins suivant l'appréciation des autorités européennes de surveillance.

Les Orientations sont jointes en annexe à la présente circulaire. Elles peuvent également être consultées sur les sites Internet des autorités européennes de surveillance, dont p.ex. le site de l'EBA à l'adresse suivante :
http://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf, en anglais,
ou à l'adresse https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_FR_04-01-2018.pdf, en français.

Veuillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments très distingués.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Jean-Pierre FABER	Françoise KAUTHEN	Claude SIMON	Claude MARX
Directeur	Directeur	Directeur	Directeur général

Annexes

JC 2017 37

04/01/2018

Orientations finales

Orientations communes, au titre des articles 17 et 18, paragraphe 4, de la directive (UE) 2015/849, sur les mesures de vigilance simplifiées et renforcées à l'égard de la clientèle et sur les facteurs que les établissements de crédit et les établissements financiers devraient prendre en considération lorsqu'ils évaluent les risques de blanchiment de capitaux et de financement du terrorisme associés aux relations d'affaires individuelles et aux transactions conclues à titre occasionnel.

Orientations sur les facteurs de risque

Obligations de conformité et de déclaration

Statut des présentes orientations communes

Le présent document contient des orientations communes émises en vertu des articles 16 et 56, premier alinéa, du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission, du règlement (UE) nº 1094/2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), ainsi que du règlement (UE) nº 1095/2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers) [ci-après les «règlements relatifs aux autorités européennes de surveillance (AES)»]. Conformément à l'article 16, paragraphe 3, des règlements AES, les autorités compétentes et les établissements financiers doivent tout mettre en œuvre pour respecter les orientations.

Les orientations communes exposent l'avis des autorités européennes de surveillance sur des pratiques de surveillance appropriées au sein du système européen de surveillance financière ou sur les modalités d'application du droit de l'Union dans un domaine particulier. Les autorités compétentes qui sont soumises aux orientations communes devraient s'y conformer en les intégrant dans leurs pratiques de surveillance, selon les modalités qu'elles estiment appropriées (par exemple en modifiant leur cadre juridique ou leurs procédures de surveillance), y compris lorsque les orientations communes s'adressent principalement à des établissements.

Obligations de déclaration

Conformément à l'article 16, paragraphe 3, des règlements AES, les autorités compétentes doivent indiquer à l'AES concernée si elles respectent ou entendent respecter les présentes orientations, ou indiquer les raisons de leur non-respect, le cas échéant, pour le 05/03/2018 au plus tard [*délai de deux mois suivant la publication de toutes les traductions sur les sites Internet des AES*.] En l'absence d'une notification dans ce délai, les autorités compétentes seront considérées par l'AES concernée comme n'ayant pas respecté les orientations. Les notifications sont à adresser à [compliance@eba.europa.eu, compliance@eiopa.europa.eu et compliance@esma.europa.eu], en indiquant en objet «JC/GL/2017/37». Un modèle de notification est disponible sur les sites Internet des AES. Les notifications devraient être communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes.

Conformément à l'article 16, paragraphe 3, les notifications seront publiées sur les sites Internet des AES.

Titre I — Objet, champ d'application et définitions

Objet

1. Les présentes orientations exposent les facteurs que les établissements devraient prendre en considération lorsqu'ils évaluent le risque de blanchiment de capitaux et de financement du terrorisme (BC/FT) associé à une relation d'affaires ou à une transaction conclue à titre occasionnel. Elles expliquent aussi comment les établissements devraient adapter l'étendue des mesures de vigilance qu'ils prennent à l'égard de la clientèle, de façon à ce que celles-ci soient proportionnées au risque de blanchiment de capitaux et de financement du terrorisme identifié par les établissements.
2. Les présentes orientations portent sur l'évaluation des risques liés aux relations d'affaires individuelles et aux transactions conclues à titre occasionnel, mais les établissements peuvent les utiliser *mutatis mutandis* lorsqu'ils évaluent les risques de BC/FT auxquels ils sont exposés dans leurs activités, conformément à l'article 8 de la directive (UE) 2015/849.
3. Les facteurs et les mesures énoncés dans les présentes orientations ne sont pas exhaustifs, et les établissements devraient prendre en compte, au besoin, d'autres facteurs et mesures.

Champ d'application

4. Les présentes orientations s'adressent aux établissements de crédit et aux établissements financiers tels que définis à l'article 3, paragraphes 1 et 2, de la directive (UE) 2015/849, ainsi qu'aux autorités compétentes chargées de surveiller le respect par ces établissements de leurs obligations en matière de lutte contre le BC/FT.
5. Les autorités compétentes devraient utiliser les présentes orientations lorsqu'elles évaluent l'adéquation des évaluations de risques et des politiques et procédures mises en place par les établissements pour lutter contre le BC/FT.
6. Les autorités compétentes devraient également déterminer dans quelle mesure les présentes orientations peuvent éclairer l'évaluation du risque de BC/FT associé à leur secteur, laquelle s'inscrit dans le cadre de l'approche de la surveillance fondée sur les risques. Les AES ont publié des orientations sur la surveillance fondée sur les risques conformément à l'article 48, paragraphe 10, de la directive (UE) 2015/849.
7. Le respect du régime européen en matière de sanctions financières ne relève pas du champ d'application des présentes orientations.

Définitions

8. Les définitions suivantes s'appliquent aux fins des présentes orientations:

- on entend par «autorités compétentes», les autorités compétentes pour veiller à ce que les établissements se conforment aux exigences de la directive (UE) 2015/849 telle que transposée en droit national[1].
- On entend par «établissements», les établissements de crédit et les établissements financiers tels que définis à l'article 3, paragraphes 1 et 2, de la directive (UE) 2015/849.

On entend par «pays ou territoires associés à un risque plus élevé de BC/FT», les pays ou territoires qui, sur la base d'une évaluation des facteurs de risques énoncés au titre II des présentes orientations, présentent un risque plus élevé de blanchiment de capitaux et de financement du terrorisme. Ce terme inclut notamment les «pays tiers à haut risque» dont les dispositifs de lutte contre le BC/FT sont identifiés comme présentant des carences stratégiques qui font peser une menace significative sur le système financier de l'Union [article 9 de la directive (UE) 2015/849].

- On entend par «transaction conclue à titre occasionnel», une transaction qui n'est pas exécutée dans le cadre d'une relation d'affaires telle que définie à l'article 3, paragraphe 13, de la directive (UE) 2015/849.
- On entend par «compte commun» [pooled account], un compte bancaire ouvert par un client, par exemple un avocat ou un notaire, en vue de la détention des avoirs de ses clients. Les fonds des clients seront mis en commun, mais les clients ne pourront pas directement donner l'ordre à la banque d'exécuter des transactions.
- On entend par «risque», l'incidence et la probabilité de la survenue du risque de BC/FT. Le risque se rapporte au risque inhérent, c'est-à-dire au niveau de risque qui existe avant toute atténuation. Il ne se rapporte pas au risque résiduel, c'est-à-dire au niveau de risque qui demeure après toute atténuation.
- On entend par «facteurs de risques», les variables qui, isolément ou ensemble, peuvent augmenter ou diminuer le risque de BC/FT que pose une relation d'affaires individuelle ou une transaction conclue à titre occasionnel.
- On entend par «approche fondée sur les risques», une approche par laquelle les autorités compétentes et les établissements identifient, évaluent et comprennent les risques de BC/FT auxquels les établissements sont exposés et prennent des mesures de lutte contre le BC/FT qui sont proportionnées à ces risques.
- On entend par «origine des fonds», l'origine des fonds impliqués dans une relation d'affaires ou une transaction conclue à titre occasionnel. Cela comprend aussi bien l'activité ayant généré les fonds utilisés dans la relation d'affaires, par exemple le salaire du client, que les moyens utilisés pour transférer les fonds du client.

[1] Article 4, paragraphe 2, sous ii), du règlement (UE) nº 1093/2010, article 4, paragraphe 2, sous ii), du règlement (UE) nº 1094/2010 et article 4, paragraphe 3, sous ii), du règlement (UE) nº 1093/2010.

- On entend par «origine du patrimoine», l'origine du patrimoine total du client, par exemple un héritage ou la constitution d'une épargne.

Titre II – Évaluation et gestion du risque: considérations générales

9. Les présentes orientations se divisent en deux parties. Le titre II est général et s'applique à tous les établissements. Le titre III expose des orientations spécifiques à certains secteurs. Le titre III est incomplet lorsqu'il est pris isolément et devrait être lu conjointement avec le titre II.

10. L'approche des établissements en matière d'évaluation et de gestion du risque de blanchiment de capitaux et de financement du terrorisme associé aux relations d'affaires et aux transactions conclues à titre occasionnel devrait inclure les éléments suivants:

- Évaluations des risques à l'échelle de l'entreprise.

  Les évaluations de risques à l'échelle de l'entreprise devraient aider les établissements à identifier les domaines dans lesquels ils sont exposés à un risque de BC/FT et les secteurs de leurs activités sur lesquels ils devraient concentrer la LCB/FT. À cet effet, et conformément à l'article 8 de la directive (UE) 2015/849, les établissements devraient identifier et évaluer le risque de BC/FT associé aux produits et aux services qu'ils proposent, aux pays ou territoires dans lesquels ils opèrent, aux clients qu'ils attirent, ainsi qu'aux canaux de transaction ou de distribution qu'ils utilisent pour servir leurs clients. Les mesures prises par les établissements pour identifier et évaluer le risque de blanchiment de capitaux et de financement du terrorisme auquel ils sont exposés dans leurs activités doivent être proportionnées à la nature et à la taille de chaque établissement. Les établissements qui ne proposent pas de produits ou de services complexes et présentent une exposition internationale limitée, voire nulle, pourraient ne pas avoir besoin d'une évaluation des risques trop complexe ou trop sophistiquée.

- Mesures de vigilance à l'égard de la clientèle.

  Les établissements devraient se servir des conclusions de leur évaluation des risques pour éclairer leur décision concernant le niveau et le type de mesures de vigilance appropriés qu'ils appliqueront dans le cadre de leurs relations d'affaires individuelles et des transactions conclues à titre occasionnel.

  Avant de nouer une relation d'affaires ou d'exécuter une transaction à titre occasionnel, les établissements devraient appliquer des mesures de vigilance à l'égard de la clientèle, conformément à l'article 13, paragraphe 1, points a), b) et c), et à l'article 14, paragraphe 4, de la directive (UE) 2015/849. Les mesures de vigilance initiales à l'égard de la clientèle devraient comprendre au moins des mesures fondées sur l'appréciation des risques afin:

  i. d'identifier le client et, le cas échéant, le bénéficiaire effectif ou les représentants légaux du client;

ii. de vérifier l'identité du client sur la base de sources fiables et indépendantes et afin, le cas échéant, de vérifier l'identité du bénéficiaire effectif de telle manière que l'établissement ait l'assurance de savoir qui est le bénéficiaire effectif; et

iii. d'établir l'objet et la nature envisagée de la relation d'affaires.

Les établissements devraient adapter l'étendue des mesures de vigilance initiales à l'égard de la clientèle sur la base d'une appréciation des risques. Lorsque le risque associé à une relation d'affaires est faible, et dans la mesure où c'est autorisé par le droit national, les établissements pourraient être en mesure d'appliquer des mesures de vigilance simplifiées à l'égard de la clientèle. Lorsque le risque associé à une relation d'affaires est accru, les établissements doivent appliquer des mesures de vigilance renforcées à l'égard de la clientèle.

- Obtenir une vue globale.

  Les établissements devraient rassembler suffisamment d'informations pour s'assurer qu'ils ont identifié tous les facteurs de risque pertinents, y compris, si nécessaire, en appliquant des mesures de vigilance supplémentaires à l'égard de la clientèle, et ils devraient évaluer ces facteurs de risque afin d'obtenir une vue globale du risque associé à une relation d'affaires ou à une transaction occasionnelle particulière. Les établissements devraient garder à l'esprit que les facteurs de risque énumérés dans les présentes orientations ne sont pas exhaustifs, et que les établissements ne sont pas tenus de prendre en considération tous les facteurs de risque dans tous les cas.

- Contrôle et réexamen.

  Les établissements doivent tenir à jour et réexaminer régulièrement leur évaluation des risques[2]. Les établissements doivent contrôler les transactions pour s'assurer qu'elles soient cohérentes par rapport au profil de risque et aux activités commerciales du client. Ils doivent, si nécessaire, examiner l'origine des fonds pour détecter d'éventuels cas de BC/FT. Ils doivent également tenir à jour les documents, données et informations dont ils disposent afin de déterminer si le risque associé à la relation d'affaires a changé[3].

Évaluations des risques: méthodologie et facteurs de risque

11. Une évaluation des risques devrait s'articuler autour de deux étapes distinctes mais liées:

    a. l'identification du risque de BC/FT; et

    b. l'évaluation du risque de BC/FT.

[2] Article 8, paragraphe 2, de la directive (UE) 2015/849.

[3] Article 13, paragraphe 1, point d), de la directive (UE) 2015/849.

Identifier le risque de blanchiment de capitaux et de financement du terrorisme

12. Les établissements devraient recenser les risques de BC/FT auxquels ils sont (ou seraient) exposés lorsqu'ils nouent une relation d'affaires ou concluent une transaction à titre occasionnel.

13. Lorsqu'ils identifient les risques de BC/FT associés à une relation d'affaires ou à une transaction conclue à titre occasionnel, les établissements devraient considérer les facteurs de risque pertinents, et notamment les caractéristiques de leur client, les pays ou zones géographiques dans lesquels ils opèrent, les produits, services et transactions spécifiques demandés par le client, et les canaux utilisés par l'établissement pour fournir ces produits, services et transactions.

Sources d'information

14. Les informations relatives à ces facteurs de risque de BC/FT devraient, si possible, provenir de sources variées, qu'elles soient accessibles individuellement ou au moyen d'outils ou de bases de données qui sont disponibles dans le commerce et qui rassemblent des informations provenant de sources multiples. Les établissements devraient déterminer le type et le nombre de sources sur la base d'une appréciation des risques.

15. Les établissements devraient toujours prendre en considération les sources d'information suivantes:

- l'évaluation supranationale des risques effectuée par la Commission européenne;
- les informations émanant des pouvoirs publics, telles que les évaluations nationales des risques, les déclarations et alertes émises par les autorités, ainsi que les notes d'explication concernant la législation applicable;
- les informations des régulateurs, telles que les orientations et les raisonnements exposés dans les amendes réglementaires;
- les informations communiquées par les cellules de renseignement financier (CRF) et les autorités répressives, telles que les rapports sur les menaces, les alertes et les typologies; et
- les informations obtenues dans le cadre du processus de mesures de vigilance à l'entrée en relations d'affaires à l'égard de la clientèle.

16. Les autres sources d'information qui peuvent être envisagées par les établissements dans ce contexte peuvent notamment comprendre:

- les propres connaissances et l'expertise professionnelle de l'établissement;
- les informations émanant d'organismes professionnels, telles que les typologies et les risques émergents;
- les informations provenant de la société civile, telles que les indices de corruption et les rapports sur les pays;

- les informations émanant des organes chargés de l'élaboration de normes internationales, telles que les rapports d'évaluations mutuelles ou les listes noires juridiquement non contraignantes;
- les informations provenant de sources crédibles et fiables, telles que les rapports publiés dans des journaux réputés;
- les informations émanant d'organisations commerciales crédibles et fiables, telles que les rapports sur les risques et les rapports de renseignement; et
- les informations émanant d'organisations statistiques et du monde universitaire.

Facteurs de risque

17. Les établissements devraient garder à l'esprit que les facteurs de risque suivants ne sont pas exhaustifs, et qu'ils ne sont pas tenus de prendre en considération tous les facteurs de risque dans tous les cas. Les établissements devraient avoir une vue globale du risque lié à la situation et garder à l'esprit que, à moins que la directive (UE) 2015/849 ou le droit national n'en dispose autrement, la présence de facteurs de risque isolés ne signifie pas nécessairement qu'une relation doive être classée dans une catégorie de risque plus élevée ou plus faible.

Facteurs de risque liés aux clients

18. Lorsqu'ils identifient le risque associé à leurs clients, y compris aux bénéficiaires effectifs de leurs clients,[4] les établissements devraient prendre en compte le risque lié:

    a. aux activités commerciales ou professionnelles du client et du bénéficiaire effectif du client;

    b. à la réputation du client et du bénéficiaire effectif du client;

    c. à la nature et au comportement du client et du bénéficiaire effectif du client.

19. Les facteurs de risque qui peuvent être pertinents lors de la prise en compte du risque associé aux activités commerciales ou professionnelles d'un client ou du bénéficiaire effectif d'un client comprennent notamment:

- Le client ou le bénéficiaire effectif a-t-il des liens avec des secteurs qui sont communément associés à un risque de corruption plus élevé, tels que le bâtiment, le secteur pharmaceutique et la santé, l'industrie de l'armement et la défense, les industries extractives et la passation de marchés publics?
- Le client ou le bénéficiaire effectif a-t-il des liens avec des secteurs qui sont associés à un risque plus élevé de BC/FT, par exemple certains prestataires de services monétaires, les casinos et les négociants de métaux précieux?

[4] Pour plus d'informations sur les facteurs de risque associés aux bénéficiaires de contrats d'assurance vie, veuillez vous reporter au titre III, chapitre 7.

- Le client ou le bénéficiaire effectif a-t-il des liens avec des secteurs qui impliquent d'importants montants en espèces?
- Lorsque le client est une personne morale ou une construction juridique, quel son objet social? Par exemple, quelle est la nature de son activité?
- Le client a-t-il des liens politiques? S'agit-il par exemple d'une personne politiquement exposée (PPE), ou son bénéficiaire effectif est-il une PPE? Le client ou le bénéficiaire effectif a-t-il d'autres liens pertinents avec une PPE, par exemple les directeurs du client sont-ils des PPE et, si oui, ces dernières exercent-elles un contrôle significatif sur le client ou le bénéficiaire effectif? Lorsqu'un client ou son bénéficiaire effectif est une PPE, les établissements doivent toujours appliquer des mesures de vigilance renforcées à l'égard de la clientèle, conformément à l'article 20 de la directive (UE) 2015/849.
- Le client ou le bénéficiaire effectif exerce-t-il une autre fonction importante ou jouit-il d'une notoriété publique qui pourrait lui permettre d'abuser de cette fonction en vue d'un gain personnel? Par exemple, s'agit-il d'un haut fonctionnaire local ou régional ayant la capacité d'influencer l'attribution de marchés publics, de décideurs d'organismes sportifs influents ou d'individus connus pour leur influence sur le gouvernement et sur d'autres décideurs de haut niveau?
- Le client est-il une personne morale qui est soumise à des obligations contraignantes de déclaration qui garantissent que des informations fiables concernant le bénéficiaire effectif du client sont accessibles au public, par exemple une société cotée sur un marché boursier qui exige une telle déclaration comme condition d'admission à la cote?
- Le client est-il un établissement de crédit ou un établissement financier agissant pour son propre compte dans un pays ou territoire doté d'un dispositif efficace de lutte contre le BC/FT, et fait-il l'objet d'une surveillance en ce qui concerne le respect des obligations locales en matière de lutte contre le BC/FT? Existe-t-il des preuves que le client a fait l'objet au cours des dernières années de sanctions ou de mesures répressives de la part d'un organisme de supervision en raison du non-respect d'obligations de lutte contre le BC/FT ou d'exigences de comportement plus générales?
- Le client est-il une administration ou une entreprise publique d'un pays ou territoire présentant de faibles niveaux de corruption?
- Les informations sur le client ou le bénéficiaire effectif correspondent-elles à ce que l'établissement sait de leurs activités commerciales précédentes, actuelles ou envisagées, du chiffre d'affaires, de l'origine des fonds ou de l'origine de leur patrimoine?

20. Les facteurs de risque suivants peuvent être pertinents lors de la prise en compte du risque associé à la réputation d'un client ou d'un bénéficiaire effectif:

- Existe-t-il des échos négatifs dans les médias ou d'autres sources d'information pertinentes concernant le client, par exemple le client ou le bénéficiaire effectif est-il accusé d'actes criminels ou terroristes? Si oui, ces informations sont-elles fiables et crédibles? Les

établissements devraient déterminer la crédibilité des allégations rapportées dans les médias en fonction notamment de la qualité et de l'indépendance de la source d'information et de la persistance de ces informations dans les médias. Les établissements devraient garder à l'esprit que l'absence de condamnations pénales ne suffit pas, seule, à écarter les allégations d'infractions.

- Le client, le bénéficiaire effectif ou toute personne connue publiquement pour être étroitement associée à ceux-ci a-t-il vu ses avoirs gelés en raison d'une procédure administrative ou pénale ou d'accusations en matière de terrorisme ou de financement du terrorisme? L'établissement a-t-il des motifs raisonnables de soupçonner que le client, le bénéficiaire effectif ou toute personne connue publiquement pour être étroitement associée à ceux-ci a fait l'objet, à un quelconque moment dans le passé, d'un tel gel d'avoirs?
- L'établissement sait-il si le client ou le bénéficiaire effectif a fait l'objet par le passé d'une déclaration de transaction suspecte?
- L'établissement dispose-t-il d'informations internes concernant l'intégrité du client ou du bénéficiaire effectif qu'il aurait obtenues, par exemple, dans le cadre d'une relation d'affaires de longue date?

21. Les facteurs de risque suivants peuvent être pertinents lors de la prise en compte du risque associé à la nature et au comportement d'un client ou d'un bénéficiaire effectif; les établissements devraient noter que certains de ces facteurs de risque ne seront pas perceptibles d'emblée et pourraient n'apparaître qu'après l'établissement d'une relation d'affaires:

- Le client a-t-il des motifs légitimes de ne pas être en mesure de fournir des preuves solides de son identité, peut-être parce qu'il s'agit d'un demandeur d'asile?[5]
- L'établissement a-t-il des doutes concernant la véracité ou l'exactitude de l'identité du client ou du bénéficiaire effectif?
- Existe-t-il des indices selon lesquels le client pourrait chercher à éviter l'établissement d'une relation d'affaires? Par exemple, le client cherche-t-il à exécuter une seule transaction ou plusieurs transactions isolées alors que l'établissement d'une relation d'affaires pourrait être plus logique sur le plan économique?
- La structure de propriété et de contrôle du client est-elle transparente et logique? Si la structure de propriété et de contrôle du client est complexe ou opaque, existe-t-il une justification commerciale ou licite évidente?
- Le client émet-il des actions au porteur ou son capital est-il détenu par des actionnaires nominatifs (*nominee shareholders*)?

[5] L'ABE a publié un «Avis sur l'application de mesures de vigilance à l'égard de la clientèle aux clients qui sont des demandeurs d'asile issus de pays ou de territoires tiers à haut risque», voir https://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+client+Due+Diligence+on+Asylum+Seekers%29.pdf.

- Le client est-il une personne morale ou une construction juridique qui pourrait être utilisée comme une structure de détention d'actifs?
- Existe-t-il une raison valable aux modifications apportées à la structure de propriété et de contrôle du client? Le client demande-t-il des transactions complexes, d'un montant inhabituellement ou anormalement élevé, ou des types inhabituels ou inattendus de transaction, n'ayant pas d'objet économique ou licite apparent ou de justification commerciale valable? Existe-t-il des raisons de soupçonner que le client tente d'échapper à des seuils spécifiques, tels que ceux visés à l'article 11, point b), de la directive (UE) 2015/849, et à la législation nationale, le cas échéant?
- Le client exige-t-il des niveaux de secret professionnel inutiles ou déraisonnables? Par exemple, le client est-il peu enclin à communiquer des informations dans le cadre du processus de vigilance à l'égard de la clientèle, ou semble-t-il vouloir masquer la véritable nature de ses activités?
- L'origine du patrimoine ou l'origine des fonds du client ou du bénéficiaire effectif peut-elle être facilement expliquée, par exemple au regard de la profession, de l'héritage ou des placements du client ou du bénéficiaire effectif? Cette explication est-elle plausible?
- Le client utilise-t-il les produits et les services qu'il a souscrits de la manière annoncée lors de l'établissement initial de la relation d'affaires?
- Lorsque le client est un non résident, ses besoins pourraient-ils être mieux servis ailleurs? Le client a-t-il des motifs économiques et légaux valables pour demander le type de service financier souhaité? Les établissements devraient noter que l'article 16 de la directive 2014/92/UE instaure le droit pour les clients résidant légalement dans l'Union d'accéder à un compte de paiement de base, mais que ce droit n'est applicable que dans la mesure où les établissements de crédit peuvent respecter leurs obligations de lutte contre le BC/FT[6].
- Le client est-il un organisme à but non lucratif dont les activités pourraient être détournées à des fins de financement du terrorisme?

Pays et zones géographiques

22. Lorsqu'ils identifient le risque associé aux pays et zones géographiques, les établissements devraient prendre en considération le risque lié:

    a. aux pays ou territoires dans lesquels le client et le bénéficiaire effectif sont installés;

    b. aux pays ou territoires dans lesquels le client et le bénéficiaire effectif ont leur activité et siège;

    c. aux pays ou territoires avec lesquels le client et le bénéficiaire effectif ont des liens personnels effectifs.

[6] Voir, en particulier, l'article premier, paragraphe 7, et l'article 16, paragraphe 4, de la directive 2014/92/UE.

23. Les établissements devraient noter que la nature et l'objet de la relation d'affaires déterminent souvent l'importance relative des facteurs de risque liés aux différents pays et zones géographiques (voir également les points 36 à 38). Par exemple:

- Lorsque les fonds utilisés dans la relation d'affaires ont été générés à l'étranger, le niveau des infractions sous-jacentes au blanchiment de capitaux et l'efficacité du système juridique du pays concerné devront plus particulièrement être pris en compte.
- Lorsque les fonds sont reçus de, ou envoyés vers des pays ou territoires dans lesquels opèrent des groupes qui sont connus pour commettre des infractions terroristes, les établissements devraient envisager dans quelle mesure cela pourrait faire naître un soupçon, en fonction de ce que l'établissement sait de l'objet et de la nature de la relation d'affaires.
- Lorsque le client est un établissement de crédit ou un établissement financier, les établissements devraient accorder une attention particulière à l'adéquation du dispositif de lutte du pays contre le BC/FT, ainsi qu'à l'efficacité de la surveillance en matière de lutte contre le BC/FT.
- Lorsque le client est une structure juridique ou une fiducie/un trust, les établissements devraient prendre en compte la mesure dans laquelle le pays dans lequel le client et, le cas échéant, le bénéficiaire effectif sont immatriculés respecte effectivement les normes internationales en matière de transparence fiscale.

24. Les facteurs de risque que les établissements devraient prendre en considération lorsqu'ils identifient l'efficacité du dispositif de lutte contre le BC/FT d'un pays ou territoire portent notamment sur les aspects suivants:

- Le pays a-t-il été identifié par la Commission comme un pays dont le dispositif de lutte contre le BC/FT présente des carences stratégiques, conformément à l'article 9 de la directive (UE) 2015/849? Lorsque les établissements entrent en relation d'affaires avec des personnes physiques ou morales résidant ou établies dans des pays tiers que la Commission a identifiés comme présentant un risque élevé de BC/FT, ils doivent toujours appliquer des mesures de vigilance renforcées à l'égard de la clientèle[7].
- Existe-t-il des informations provenant de plusieurs sources crédibles et fiables concernant la qualité des contrôles du pays ou territoire en matière de lutte contre le BC/FT, y compris des informations sur la qualité et l'efficacité de l'application de la réglementation et de la surveillance réglementaire? Les sources d'information possibles comprennent, par exemple, les rapports d'évaluation du Groupe d'action financière internationale (GAFI) ou des organismes régionaux de type GAFI (ORTG) (la synthèse, les principales conclusions et l'évaluation du respect des recommandations 10, 26 et 27 et des résultats immédiats 3 et 4 constituent un bon point de départ), la liste GAFI des pays ou territoires à haut risque et non coopératifs, les évaluations du Fonds monétaire international (FMI), ainsi que les rapports du Programme d'évaluation du secteur financier (FSAP). Les établissements devraient garder à l'esprit que

[7] Article 18, paragraphe 1, de la directive (UE) 2015/849.

l'adhésion au GAFI ou à un ORTG (MoneyVal, par exemple) ne signifie pas, en soi, que le dispositif de lutte contre le BC/FT du pays ou territoire est adéquat et efficace.

Les établissements devraient noter que la directive (UE) 2015/849 ne reconnaît pas l'«équivalence» des pays tiers, et que les listes de pays ou territoires équivalents des États membres de l'UE ne sont plus tenues à jour. Dans la mesure où cela est autorisé par le droit national, les établissements devraient être en mesure d'identifier les pays présentant un risque moins élevé conformément aux présentes orientations et à l'annexe II de la directive (UE) 2015/849.

25. Les facteurs de risque que les établissements devraient prendre en considération lorsqu'ils identifient le niveau de risque de financement du terrorisme associé à un pays ou territoire comprennent:

- Existe-t-il des informations provenant, par exemple, d'autorités répressives ou de sources médiatiques crédibles et fiables, indiquant qu'un pays finance ou soutient des activités terroristes ou que des groupes commettant des infractions terroristes sont connus pour opérer dans le pays ou territoire?
- Le pays ou territoire fait-il l'objet de sanctions financières, d'embargos ou de mesures liées au terrorisme, au financement du terrorisme ou à la prolifération imposés, par exemple, par les Nations unies ou par l'Union européenne?

26. Les facteurs de risque que les établissements devraient prendre en considération lorsqu'ils identifient le niveau de transparence et de respect des obligations fiscales d'un pays ou territoire portent notamment sur les aspects suivants:

- Existe-t-il des informations provenant de plusieurs sources crédibles et fiables selon lesquelles le pays a été considéré comme respectant les normes internationales en matière de transparence fiscale et d'échange d'informations? Existe-t-il des preuves selon lesquelles les règles adéquates sont effectivement mises en œuvre dans la pratique? Les sources d'information possibles comprennent notamment les rapports du Forum mondial sur la transparence et l'échange de renseignements de l'Organisation de coopération et de développement économiques (OCDE), qui classent les pays ou territoires à des fins de transparence fiscale et d'échange d'informations; les évaluations de l'engagement du pays ou du territoire en faveur de l'échange automatique de renseignements sur la base de la Norme commune de déclaration (CRS); les évaluations du respect des recommandations 9, 24 et 25 du GAFI et des résultats immédiats 2 et 5 du GAFI ou des ORTG; et les évaluations du FMI (par exemple, les évaluations des centres financiers offshore par le personnel du FMI).
- Le pays ou territoire s'est-il engagé à respecter, et a-t-il effectivement mis en œuvre la Norme commune de déclaration sur l'échange automatique de renseignements, adoptée par le G20 en 2014?
- Le pays ou le territoire a-t-il mis en place des registres de bénéficiaires effectifs fiables et accessibles?

27. Les facteurs de risque que les établissements devraient prendre en considération lorsqu'ils identifient le risque associé au niveau d'infractions sous-jacentes au blanchiment de capitaux comprennent:

- Existe-t-il des informations provenant de sources crédibles et fiables concernant le niveau des infractions sous-jacentes au blanchiment de capitaux énumérées à l'article 3, paragraphe 4, de la directive (UE) 2015/849, telles que la corruption, la criminalité organisée, les infractions fiscales pénales ou la fraude grave? On peut citer par exemple les indices de perception de la corruption, les rapports sur les pays de l'OCDE concernant la mise en œuvre de la convention de l'OCDE contre la corruption, et le rapport de l'Office des Nations Unies contre la drogue et le crime.
- Existe-t-il des informations provenant de plusieurs sources crédibles et fiables concernant la capacité du système judiciaire et d'enquête du pays à rechercher et à poursuivre efficacement ces infractions?

Facteurs de risque liés aux produits, aux services et aux transactions

28. Lorsqu'ils identifient le risque associé à leurs produits, services et transactions, les établissements devraient prendre en considération le risque lié:

    a. au niveau de transparence, ou d'opacité, offert par le produit, le service ou la transaction;

    b. à la complexité du produit, du service ou de la transaction; et

    c. à la valeur ou à la taille du produit, du service ou de la transaction.

29. Les facteurs de risque qui peuvent être pertinents pour évaluer le risque associé à la transparence d'un produit, d'un service ou d'une transaction comprennent:

- Dans quelle mesure les produits ou services permettent-ils au client, au bénéficiaire effectif ou aux structures bénéficiaires de rester anonymes ou de masquer leur identité plus facilement? Ces produits et services comprennent notamment les actions au porteur, les placements fiduciaires, les véhicules offshore et certain(e)s fiducies/trusts, ainsi que les entités juridiques telles que les fondations, qui peuvent être structurées de façon à profiter de l'anonymat et permettent de conclure des transactions avec des sociétés écrans ou des sociétés dont le capital est détenu par des actionnaires apparents.
- Dans quelle mesure est-il possible pour un tiers ne faisant pas partie de la relation d'affaires de donner des instructions, par exemple dans le cas de certaines relations de correspondance bancaire?

30. Les facteurs de risque qui peuvent être pertinents pour évaluer le risque associé à la complexité d'un produit, d'un service ou d'une transaction comprennent:

- Dans quelle mesure la transaction est-elle complexe, et implique-t-elle plusieurs parties ou plusieurs pays ou territoires, par exemple dans le cas de certaines opérations de financement

du commerce? Les transactions sont-elles simples? Par exemple des versements réguliers sont-ils effectués sur un fonds de pension?

- Dans quelle mesure les produits ou services permettent-ils les paiements par des tiers ou acceptent-ils les paiements excédentaires lorsque cela n'est pas normalement prévu? Lorsque des paiements de tiers sont prévus, l'établissement connaît-il l'identité du tiers, par exemple s'agit-il d'une autorité chargée du paiement d'allocations publiques ou d'un garant? Ou les produits et services sont-ils financés exclusivement au moyen de transferts de fonds depuis le compte du client vers un autre établissement financier qui est soumis à des normes et à une surveillance en matière de lutte contre le BC/FT qui sont comparables à celles requises en application de la directive (UE) 2015/849?
- L'établissement comprend-il les risques associés à son produit ou service lorsque celui-ci est nouveau ou innovant, en particulier lorsque cela implique le recours à des technologies ou des méthodes de paiement nouvelles?

31. Les facteurs de risque qui peuvent être pertinents pour évaluer le risque associé à la valeur ou au montant d'un produit, d'un service ou d'une transaction comprennent:

- Dans quelle mesure les produits ou services impliquent-ils beaucoup d'espèces, à l'instar de nombreux services de paiement mais aussi de certains comptes courants?
- Dans quelle mesure les produits ou services facilitent-ils ou favorisent-ils des transactions d'un montant élevé? Existe-t-il des plafonds sur les montants des transactions ou sur les niveaux de primes qui pourraient limiter l'utilisation du produit ou du service à des fins de blanchiment de capitaux et de financement du terrorisme?

Facteurs de risque liés aux canaux de distribution

32. Lorsqu'ils analysent le risque associé à la façon dont le client obtient les produits ou services dont il a besoin, les établissements devraient prendre en compte le risqué lié:

    a. au fait que la relation d'affaires est conduite sans la présence physique des parties; et

    b. aux apporteurs d'affaires ou aux intermédiaires auxquels l'établissement pourrait avoir recours, ainsi qu'à la nature de leur relation avec l'établissement.

33. Lorsqu'ils évaluent le risque associé à la façon dont le client obtient les produits ou services, les établissements devraient prendre en compte un certain nombre de facteurs, et notamment ceux qui suivent:

- Le client est-il présent physiquement à des fins d'identification? Si le client n'est pas présent physiquement, l'établissement a-t-il eu recours à une forme fiable de mesures de vigilance à l'égard de la clientèle n'impliquant pas la présence physique des parties? A-t-il pris des mesures pour éviter l'usurpation ou la fraude à l'identité?
- Le client a-t-il été introduit par une autre partie appartenant au même groupe financier et, si tel est le cas, dans quelle mesure l'établissement peut-il s'appuyer sur cette mise en relation

pour avoir la garantie que le client ne l'exposera pas à un risque excessif de BC/FT? Quelles mesures l'établissement a-t-il prises pour s'assurer que le groupe applique des mesures de vigilance à l'égard de la clientèle qui répondent aux normes de l'Espace économique européen (EEE), conformément à l'article 28 de la directive (UE) 2015/849?

- Le client a-t-il été introduit par un tiers, par exemple une banque n'appartenant pas au même groupe? Ce tiers est-il un établissement financier ou bien ses principales activités commerciales n'ont-elles aucun lien avec la fourniture de services financiers? Quelles mesures l'établissement a-t-il prises pour s'assurer:

    i. que le tiers applique des mesures de vigilance à l'égard de la clientèle et conserve des documents conformément aux normes de l'EEE, et qu'il fait l'objet d'une surveillance concernant le respect d'obligations comparables en matière de lutte contre le BC/FT, conformément à l'article 26 de la directive (UE) 2015/849;

    ii. que le tiers fournira immédiatement sur demande des copies pertinentes des données d'identification et de vérification, conformément notamment à l'article 27 de la directive (UE) 2015/849; et

    iii. que la qualité des mesures de vigilance prises par le tiers à l'égard de la clientèle est telle que l'on peut s'appuyer sur elle?

- Le client a-t-il été introduit par un agent lié, c'est-à-dire sans contact direct avec l'établissement? Dans quelle mesure l'établissement peut-il s'assurer que l'agent a obtenu suffisamment d'informations pour que l'établissement puisse connaître son client et le niveau de risque associé à la relation d'affaires?
- Si l'établissement a recours à des agents indépendants ou liés, dans quelle mesure ceux-ci sont-ils impliqués sur une base continue dans la conduite des affaires? Quelle incidence cela a-t-il sur la connaissance du client et la gestion continue des risques par l'établissement?
- Lorsqu'un établissement a recours à un intermédiaire:

    i. L'intermédiaire est-il une personne réglementée soumise à des obligations de lutte contre le blanchiment de capitaux qui sont compatibles avec celles prévues par la directive (UE) 2015/849?

    ii. L'intermédiaire fait-il l'objet d'une surveillance efficace en matière de lutte contre le blanchiment de capitaux? Existe-t-il des indices selon lesquels le niveau de respect par l'intermédiaire de la législation ou de la réglementation applicable en matière de lutte contre le blanchiment de capitaux est inadéquat, par exemple l'intermédiaire a-t-il été sanctionné pour des infractions aux obligations de lutte contre le BC/FT?

L'intermédiaire est-il établi dans un pays ou territoire associé à un risque plus élevé de BC/FT? Lorsqu'un tiers est installé dans un pays tiers à haut risque que la Commission a identifié comme présentant des carences stratégiques, les établissements ne doivent pas avoir recours à cet

intermédiaire. Toutefois, dans la mesure où cela est autorisé par la droit national, il peut être possible de recourir à un tel intermédiaire à condition que celui-ci soit une succursale ou une filiale détenue majoritairement d'un autre établissement installé dans l'Union, et que l'établissement ait la certitude que l'intermédiaire respecte pleinement les politiques et procédures à l'échelle du groupe conformément à l'article 45 de la directive (UE) 2015/849[8].

Évaluation du risque de BC/FT

34. Les établissements devraient avoir une vue globale des facteurs de risque de BC/FT qu'ils ont identifiés et qui, ensemble, détermineront le niveau de risque de BC/FT associé à une relation d'affaires ou à une transaction conclue à titre occasionnel.

35. Dans le cadre de cette évaluation, les établissements peuvent décider de pondérer les facteurs différemment en fonction de leur degré d'importance

Pondération des facteurs de risque

36. Lorsqu'ils pondèrent les facteurs de risque, les établissements devraient porter un jugement éclairé sur la pertinence des différents facteurs de risque dans le cadre d'une relation d'affaires ou d'une transaction conclue à titre occasionnel. Dans ce cadre, les établissements sont souvent amenés à attribuer des «notes» différentes aux différents facteurs; par exemple, les établissements peuvent décider que les liens personnels d'un client avec un pays ou territoire associé à un risque plus élevé de BC/FT sont moins pertinents au regard des caractéristiques du produit demandé.

37. Enfin, le poids accordé à chacun de ces facteurs est susceptible de varier d'un produit à l'autre et d'un client à l'autre (ou d'une catégorie de client à l'autre) et d'un établissement à l'autre. Lorsqu'ils pondèrent les facteurs de risque, les établissements devraient veiller:

- à ce que la pondération ne soit pas influencée de manière excessive par un seul facteur;
- à ce que la notation du risque ne soit pas influencée par des considérations d'ordre économique ou de profit;
- à ce que la pondération ne crée pas à une situation dans laquelle il est impossible de classer une relation d'affaires comme présentant un risque élevé;
- à ce que la pondération de l'établissement ne puisse pas l'emporter sur les dispositions de la directive (UE) 2015/849 ou du droit national concernant les situations qui présentent toujours un risque élevé de blanchiment de capitaux; et
- à ce qu'ils puissent, si nécessaire, annuler toute notation de risque générée automatiquement. Les raisons de la décision d'annulation de ces notations devraient être documentées de manière adéquate.

[8] Article 26, paragraphe 2, de la directive (UE) 2015/849.

38. Lorsqu'un établissement utilise des systèmes informatiques automatisés pour attribuer des notations de risques globales et catégoriser des relations d'affaires ou des transactions conclues à titre occasionnel et qu'il ne conçoit pas ces systèmes en interne mais les achète auprès d'un prestataire externe, il devrait comprendre la manière dont le système fonctionne et comment le prestataire combine les facteurs de risque pour parvenir à une note de risque globale. L'établissement doit toujours être en mesure de s'assurer que les notes attribuées sont fondées sur sa compréhension du risque de BC/FT, et il devrait être en mesure d'en apporter la preuve à l'autorité compétente.

Catégorisation des relations d'affaires et des transactions conclues à titre occasionnel

39. Après avoir procédé à l'évaluation des risques, l'établissement devrait catégoriser ses relations d'affaires et les transactions conclues à titre occasionnel selon le niveau perçu du risque de BC/FT.

40. Les établissements devraient déterminer la meilleure manière de catégoriser les risques. Le mode de catégorisation choisi dépendra de la nature et de la taille de l'activité de l'établissement ainsi que des types de risques de BC/FT auxquels celui-ci est exposé. Les établissements classent souvent les risques comme élevés, moyens ou faibles, mais d'autres catégories sont possibles.

Gestion des risques: mesures de vigilance simplifiées et renforcées à l'égard de la clientèle

41. L'évaluation des risques effectuée par un établissement devrait l'aider à identifier les domaines sur lesquels il devrait concentrer ses efforts en matière de gestion des risques de BC/FT, aussi bien lors de la mise en relation avec le client que pendant la durée de la relation d'affaires.

42. A cet égard, les établissements doivent appliquer chacune des mesures de vigilance à l'égard de la clientèle prévues à l'article 13, paragraphe 1, de la directive (UE) 2015/849, mais ils peuvent déterminer l'étendue de ces mesures en fonction de leur appréciation des risques. Les mesures de vigilance à l'égard de la clientèle devraient aider les établissements à mieux comprendre le risque associé aux relations d'affaires individuelles et aux transactions conclues à titre occasionnel.

43. L'article 13, paragraphe 4, de la directive (UE) 2015/849 impose aux établissements d'être en mesure de démontrer à l'autorité compétente dont ils dépendent que les mesures de vigilance à l'égard de la clientèle qu'ils ont appliquées sont appropriées au regard des risques de BC/FT.

Mesures de vigilance simplifiées à l'égard de la clientèle

44. Dans la mesure où cela est autorisé par le droit national, les établissements peuvent appliquer des mesures de vigilance simplifiées à l'égard de la clientèle dans les situations où le risque de BC/FT associé à une relation d'affaires est évalué comme étant faible. Les mesures de vigilance

simplifiées à l'égard de la clientèle ne constituent une exemption d'aucune des mesures de vigilance à l'égard de la clientèle; toutefois, les établissements peuvent adapter leur étendue, déterminer le moment de leur mise en œuvre et le type de chacune ou de l'ensemble des mesures de vigilance à l'égard de la clientèle d'une manière qui soit proportionnée au regard du faible risque identifié.

45. Les mesures de vigilance simplifiées à l'égard de la clientèle que les établissements peuvent appliquer comprennent notamment:

- adapter le moment choisi pour appliquer les mesures de vigilance à l'égard de la clientèle, par exemple lorsque le produit ou la transaction demandé présente des caractéristiques qui en limitent l'utilisation à des fins de BC/FT par exemple:

    i. en vérifiant l'identité du client ou du bénéficiaire effectif pendant l'établissement de la relation d'affaires; ou

    ii. en vérifiant l'identité du client ou du bénéficiaire effectif dès que les transactions dépassent un seuil déterminé ou dès qu'un délai raisonnable s'est écoulé. Les établissements doivent s'assurer:

        a. que cela n'entraîne pas une exemption de facto des mesures de vigilance à l'égard de la clientèle, c'est-à-dire que les établissements doivent garantir que l'identité du client ou du bénéficiaire effectif sera vérifiée ultérieurement;

        b. que le seuil ou le délai est fixé à un niveau raisonnablement faible/court (toutefois, en ce qui concerne le financement du terrorisme, les établissements devraient noter qu'un seuil bas pourrait à lui seul ne pas être suffisant pour réduire le risque);

        c. qu'ils disposent de systèmes permettant de détecter quand le seuil ou la date limite est atteinte; et

        d. qu'ils ne reportent pas les mesures de vigilance à l'égard de la clientèle et ne retardent pas l'obtention d'informations pertinentes concernant le client lorsque la législation applicable, par exemple le règlement (UE) 2015/847, ou les dispositions du droit national exigent que ces informations soient obtenues dès le début.

- adapter la quantité d'informations obtenues à des fins d'identification, de vérification ou de contrôle, par exemple:

    i. en vérifiant l'identité sur la base des informations obtenues à partir d'un seul document ou d'une seule source de données fiable, crédible et indépendante; ou

ii. en présumant la nature et l'objet de la relation d'affaires en raison du fait que le produit est conçu exclusivement pour un usage bien précis, tel qu'un régime de retraite d'entreprise ou une carte cadeau d'un centre commercial.

- adapter la qualité ou la source des informations obtenues à des fins d'identification, de vérification ou de contrôle, par exemple:

  i. en acceptant les informations obtenues du client plutôt que d'une source indépendante lors de la vérification de l'identité du bénéficiaire effectif (il y a lieu de noter que cette modalité n'est pas autorisée pour la vérification de l'identité du client); ou

  ii. lorsque le risque associé à tous les aspects de la relation est très faible, en se fondant sur l'origine des fonds pour remplir certaines des obligations de vigilance à l'égard de la clientèle, par exemple lorsque les fonds sont des versements d'allocations publiques ou lorsque les fonds ont été transférés à partir d'un compte détenu au nom du client auprès d'un établissement de l'EEE.

- adapter la fréquence des mises à jour des mesures de vigilance à l'égard de la clientèle et des réexamens de la relation d'affaires, par exemple en les réalisant uniquement lors de la survenue d'événements déclencheurs, notamment lorsque le client souhaite souscrire un nouveau produit ou service ou qu'un certain seuil de transactions est atteint; les établissements doivent veiller à ce que cela n'entraîne pas de facto une exemption de l'obligation de tenir à jour les informations relatives aux mesures de vigilance à l'égard de la clientèle.
- adapter la fréquence et l'intensité du contrôle des transactions, par exemple en contrôlant les transactions au-delà d'un certain seuil uniquement. Lorsque les établissements choisissent de procéder de la sorte, ils doivent veiller à ce que le seuil soit fixé à un niveau raisonnable et doivent disposer de systèmes permettant de repérer les transactions liées qui, ensemble, dépasseraient ce seuil.

46. Le titre III énumère des mesures de vigilance simplifiées supplémentaires à l'égard de la clientèle qui peuvent présenter un intérêt particulier dans différents secteurs.

47. Les informations obtenues par l'établissement lors de l'application de mesures de vigilance simplifiées à l'égard de la clientèle doivent lui permettre d'obtenir l'assurance raisonnable que son analyse selon laquelle le risque associé à la relation est faible est justifiée. Elles doivent également être à même de donner suffisamment de renseignements à l'établissement concernant la nature de la relation d'affaires de façon à détecter toute transaction inhabituelle ou suspecte. Les mesures de vigilance simplifiées à l'égard de la clientèle n'exemptent pas l'établissement de l'obligation de déclarer les transactions suspectes à la CRF.

48. Lorsqu'il existe des indices selon lesquels le risque pourrait ne pas être faible, par exemple lorsqu'il existe des raisons de soupçonner qu'une tentative de BC/FT est en cours, ou lorsque l'établissement a des doutes concernant la véracité des informations obtenues, l'établissement ne doit pas appliquer de mesures de vigilance simplifiées à l'égard de la

clientèle.[9] De même, en cas de scénario spécifique à haut risque, et lorsqu'il est obligatoire de mettre en œuvre des mesures de vigilance renforcées à l'égard de la clientèle, il convient de s'abstenir d'appliquer de mesures de vigilance simplifiées à l'égard de la clientèle.

Mesures de vigilance renforcées à l'égard de la clientèle

49. Les établissements doivent appliquer des mesures de vigilance renforcées à l'égard de la clientèle dans les situations à plus haut risque, afin de gérer et d'atténuer ces risques de manière adéquate[10]. Les mesures de vigilance renforcées à l'égard de la clientèle ne peuvent se substituer aux mesures de vigilance standard à l'égard de la clientèle mais doivent au contraire être appliquées en plus de celles-ci.

50. La directive (UE) 2015/849 énumère les cas spécifiques que les établissements doivent toujours traiter comme des cas à haut risque:

    iii. lorsque le client, ou le bénéficiaire effectif du client, est une personne politiquement exposée (PPE);[11]

    iv. lorsque l'établissement noue une relation de correspondance avec un établissement client d'un pays n'appartenant pas à l'EEE;[12]

    v. lorsque l'établissement traite avec des personnes physiques ou des entités juridiques établies dans des pays tiers à haut risque;[13] et

    vi. toute transaction complexe et d'un montant inhabituellement élevé et tous les types inhabituels de transactions, n'ayant pas d'objet économique ou licite apparent.[14]

51. La directive (UE) 2015/849 expose les mesures de vigilance renforcées spécifiques que les établissements doivent appliquer à l'égard de la clientèle:

    i. lorsque le client, ou le bénéficiaire effectif du client, est une PPE;

    ii. en ce qui concerne les relations de correspondance nouées avec des établissements clients de pays tiers; et

    iii. en ce qui concerne toute transaction complexe et d'un montant inhabituellement élevé et tous les types inhabituels de transactions, n'ayant pas d'objet économique ou licite apparent.

[9] Article 11, points e) et f), et article 15, paragraphe 2, de la directive (UE) 2015/849.

[10] Articles 18 à 24 de la directive (UE) 2015/849.

[11] Articles 20 à 24 de la directive (UE) 2015/849.

[12] Article 19 de la directive (UE) 2015/849.

[13] Article 18, paragraphe 1, de la directive (UE) 2015/849.

[14] Article 18, paragraphe 2, de la directive (UE) 2015/849.

Les établissements devraient appliquer des mesures de vigilance renforcées supplémentaires à l'égard de la clientèle dans les situations où ces mesures sont appropriées au regard du risque de BC/FT qu'ils ont identifié.

Personnes politiquement exposées (PPE)

52. Les établissements qui ont identifié qu'un client ou un bénéficiaire effectif est une PPE exposée doivent toujours:

- Prendre des mesures appropriées pour établir l'origine du patrimoine et l'origine des fonds qui seront utilisés dans la relation d'affaires, afin que l'établissement puisse s'assurer qu'il ne s'agit pas du produit de la corruption ou de toute autre activité criminelle. Les mesures à prendre par les établissements pour établir l'origine du patrimoine et l'origine des fonds de la PPE dépendront du degré de risque élevé associé à la relation d'affaires. Les établissements devraient vérifier l'origine du patrimoine et l'origine des fonds sur la base de données, d'informations et de documents fiables et indépendants, lorsque le risque associé à la relation avec la PPE est particulièrement élevé.
- Obtenir d'un membre d'un niveau élevé de leur hiérarchie l'autorisation de nouer ou de maintenir une relation d'affaires avec la PPE. Le niveau hiérarchique approprié pour l'autorisation de la relation d'affaires devrait être déterminé par le niveau de risque accru associé à cette relation, et le membre d'un niveau élevé de la hiérarchie autorisant la relation d'affaires avec la PPE devrait occuper une position hiérarchique suffisamment élevée et disposer de pouvoirs de surveillance suffisants pour prendre des décisions éclairées sur des questions ayant une incidence directe sur le profil de risque de l'établissement.
- Lorsqu'il examine l'opportunité d'approuver une relation avec une PPE, le membre d'un niveau élevé de la hiérarchie devrait fonder sa décision sur le niveau de risque de BC/FT auquel l'établissement serait exposé s'il nouait cette relation d'affaires, ainsi que sur la capacité de l'établissement à gérer ce risque efficacement.
- Exercer un contrôle continu renforcé des transactions et du risque associé à la relation d'affaires. Les établissements devraient détecter les transactions inhabituelles et réexaminer régulièrement les informations dont ils disposent afin de s'assurer que toute information nouvelle ou émergente susceptible d'influencer l'évaluation des risques est identifiée en temps utile. La fréquence du contrôle continu devrait être déterminée par le niveau de risque élevé associé à la relation.

53. Les établissements doivent appliquer toutes ces mesures à l'égard des PPE, des membres de leur famille et les personnes connues pour leur être étroitement associées, et ils devraient adapter l'étendue de ces mesures en fonction de leur appréciation des risques[15].

[15] Article 20, point b), de la directive (UE) 2015/849.

Relations de correspondance

54. Les établissements doivent prendre des mesures de vigilance renforcées spécifiques à l'égard de la clientèle lorsqu'ils entretiennent une relation transfrontalière de correspondance avec un établissement client établi dans un pays tiers[16]. Les établissements doivent appliquer toutes ces mesures et devraient adapter l'étendue de celles-ci en fonction de leur appréciation des risques.

55. Les établissements devraient se référer au titre III pour ce qui concerne les orientations en matière de mesures de vigilance renforcées à l'égard de la clientèle dans le cadre des relations bancaires de correspondance; ces orientations pourraient également être utiles aux établissements dans le cadre d'autres relations de correspondance.

Transactions inhabituelles

56. Les établissements devraient mettre en place des politiques et des procédures adéquates pour détecter les transactions ou types de transactions inhabituelles. Un établissement détecte des transactions qui sont inhabituelles:

- parce qu'elles sont d'un montant plus élevé que celui auquel l'établissement pourrait normalement s'attendre compte tenu de sa connaissance du client, de la relation d'affaires ou de la catégorie à laquelle appartient le client;
- parce qu'elles présentent une forme inhabituelle ou inattendue au regard de l'activité normale du client ou du type de transactions associé à des clients, produits ou services similaires; ou
- parce qu'elles sont très complexes au regard d'autres transactions similaires associées à des types de clients, produits ou services similaires,

et que l'établissement n'a pas connaissance d'une logique économique ou d'un objet licite, ou bien qu'il doute de la véracité des informations qui lui ont été communiquées, il doit appliquer des mesures de vigilance renforcées à l'égard de la clientèle.

57. Ces mesures de vigilance renforcées à l'égard de la clientèle devraient être suffisantes pour aider l'établissement à déterminer si ces transactions font naître un soupçon, et elles doivent comprendre au moins les mesures suivantes:

- prendre des mesures raisonnables et adéquates pour comprendre le contexte et la finalité de ces transactions, par exemple en établissant l'origine et la destination des fonds ou en se renseignant sur les activités du client afin d'établir la probabilité que le client exécute de telles transactions; et
- opérer un contrôle de la relation d'affaires et les transactions ultérieures plus fréquemment et en attachant plus d'importance aux détails. L'établissement peut décider de contrôler des transactions isolément lorsque ce contrôle est proportionné au regard du risque identifié.

[16] Article 19 de la directive (UE) 2015/849.

Pays tiers à haut risque et autres situations à haut risque

58. Lorsqu'ils traitent avec des personnes physiques ou des personnes morales établies ou résidant dans un pays tiers à haut risque recensé par la Commission[17], et dans toutes les autres situations à haut risque, les établissements devraient prendre une décision éclairée pour déterminer quelles sont les mesures de vigilance renforcées à l'égard de la clientèle adaptées à chaque situation à haut risque. Le choix des mesures de vigilance renforcées appropriées à l'égard de la clientèle, y compris l'étendue des informations supplémentaires demandées, et du contrôle renforcé mis en œuvre dépendra de la raison pour laquelle une transaction conclue à titre occasionnel ou une relation d'affaires a été classée comme étant à haut risque.

59. Les établissements ne sont pas tenus d'appliquer toutes les mesures de vigilance renforcées à l'égard de la clientèle énumérées ci-dessous dans tous les cas. Par exemple, dans certaines situations à haut risque, il peut être approprié de se concentrer sur un contrôle continu renforcé pendant la durée de la relation d'affaires.

60. Les mesures de vigilance renforcées à l'égard de la clientèle que les établissements devraient appliquer peuvent comprendre:

- Augmenter la quantité d'informations obtenues aux fins des mesures de vigilance à l'égard de la clientèle:

    i. Des informations sur l'identité du client ou du bénéficiaire effectif, ou sur la structure de propriété et de contrôle du client, afin de s'assurer que le risque associé à la relation d'affaires est bien compris. Ces mesures peuvent inclure l'obtention et l'évaluation d'informations sur la réputation du client ou du bénéficiaire effectif et l'évaluation de toute allégation négative formulée à l'encontre du client ou du bénéficiaire effectif. Exemples d'informations:

        a. informations sur les membres de la famille et les personnes connues pour être étroitement associées au client ou au bénéficiaire effectif;

        b. informations sur les activités commerciales, passées et présentes, du client ou du bénéficiaire effectif; et

        c. recherches d'informations négatives dans les médias.

    ii. Informations sur la nature envisagée de la relation d'affaires pour s'assurer que la nature et l'objet de la relation d'affaires soient légitimes et pour aider les établissements à obtenir un profil de risque plus complet sur le client. Ces mesures peuvent inclure l'obtention d'informations sur:

        a. le nombre, le montant et la fréquence des transactions qui sont susceptibles de transiter par le compte, afin de permettre à l'établissement de repérer les écarts qui pourraient faire naître un soupçon (dans certains

[17] Article 9 de la directive (UE) 2015/849.

cas, il peut être utile de demander des justificatifs probants);

b. les raisons pour lesquelles le client recherche un produit ou un service précis, en particulier lorsqu'il est difficile de savoir pourquoi les besoins du client ne peuvent pas être mieux satisfaits d'une autre manière ou dans un autre pays ou territoire;

c. la destination des fonds;

d. la nature de l'activité du client ou du bénéficiaire effectif, afin de permettre à l'établissement de mieux comprendre la nature probable de la relation d'affaires.

- Augmenter la qualité des informations obtenues aux fins des mesures de vigilance à l'égard de la clientèle, afin de confirmer l'identité du client ou du bénéficiaire effectif, et notamment:

  i. en exigeant que le premier paiement soit effectué par le biais d'un compte détenu, de manière vérifiable, au nom du client auprès d'une banque soumise à des règles de vigilance à l'égard de la clientèle qui ne sont pas moins solides que celles visées au chapitre II de la directive (UE) 2015/849; ou

  ii. en s'assurant que le patrimoine et les fonds du client utilisés dans la relation d'affaires ne sont pas le produit d'activités criminelles, et que l'origine du patrimoine et l'origine des fonds correspondent à la connaissance que l'établissement a du client et de la nature de la relation d'affaires. Dans certains cas, lorsque le risque associé à la relation est particulièrement élevé, il se peut que la vérification de l'origine du patrimoine et de l'origine des fonds puisse être le seul outil adéquat pour atténuer les risques. L'origine des fonds ou du patrimoine peut être vérifiée, entre autres, à l'aide de déclarations de TVA et d'impôt sur le revenu, des copies des comptes audités, des fiches de paie, d'actes authentiques ou à des comptes rendus de médias indépendants.

- Augmenter la fréquence des réexamens pour s'assurer que l'établissement est toujours en mesure de gérer le risque associé à la relation d'affaires individuelle, ou lorsque la relation ne correspond plus à l'appétence au risque de l'établissement, pour l'aider à identifier les transactions qui nécessitent un examen plus approfondi, et notamment:

  i. en augmentant la fréquence des réexamens de la relation d'affaires pour vérifier si le profil de risque du client a changé et si le risque demeure gérable;

  ii. en obtenant d'un membre d'un niveau élevé de la hiérarchie l'autorisation de nouer ou de maintenir la relation d'affaires afin de veiller à ce que les dirigeants aient connaissance du risque auquel leur établissement est exposé et puissent prendre une décision éclairée quant à la capacité de l'établissement à gérer ce risque;

iii. en réexaminant la relation d'affaires de façon plus régulière afin de veiller à ce que tout changement dans le profil de risque du client soit identifié et évalué, et afin qu'il y soit donné suite, si nécessaire; ou

iv. en effectuant un contrôle plus fréquent ou plus approfondi des transactions afin d'identifier toute transaction inhabituelle ou inattendue qui pourrait faire naître un soupçon de BC/FT. Ce contrôle peut inclure la détermination de la destination des fonds ou la vérification des motifs des transactions.

61. Le titre III énumère les mesures de vigilance renforcées supplémentaires à l'égard de la clientèle qui pourraient présenter un intérêt particulier dans différents secteurs.

Autres considérations

62. Les établissements ne devraient pas nouer de relation d'affaires s'ils ne sont pas en mesure de respecter leurs obligations de vigilance à l'égard de la clientèle, s'ils n'ont pas l'assurance que l'objet et la nature de la relation d'affaires sont légitimes, ou s'ils n'ont pas l'assurance qu'ils peuvent gérer efficacement le risque que la relation d'affaires puisse être utilisée à des fins de BC/FT. Lorsqu'une telle relation d'affaires existe déjà, les établissements devraient y mettre un terme ou suspendre les transactions jusqu'à ce qu'ils puissent y mettre un terme, sous réserve des instructions émanant des autorités répressives, le cas échéant.

63. Lorsque les établissements ont des motifs raisonnables de soupçonner une tentative de BC/FT, ils doivent en informer leur CRF.

64. Les établissements devraient noter que l'application d'une approche par les risques ne les oblige pas, en soi, à refuser ou à mettre un terme aux relations d'affaires avec des catégories entières de clients qu'ils associent à un risque plus élevé de BC/FT, étant donné que le risque associé aux différentes relations d'affaires variera, y compris au sein d'une même catégorie.

Contrôle et réexamen

Évaluation des risques

65. Les établissements devraient réexaminer régulièrement leurs évaluations du risque de BC/FT associé aux relations d'affaires individuelles et aux transactions conclues à titre occasionnel, ainsi que des facteurs sous-jacents, afin de s'assurer que leur évaluation du risque de BC/FT est actualisée et pertinente. Les établissements devraient évaluer les informations obtenues dans le cadre du contrôle continu d'une relation d'affaires et déterminer si elles ont une incidence sur l'évaluation des risques.

66. Les établissements devraient également s'assurer qu'ils disposent de systèmes et de contrôles pour identifier les risques émergents de BC/FT, et qu'ils soient en mesure d'évaluer ces risques et, le cas échéant, de les intégrer en temps utile dans leurs évaluations individuelles et à l'échelle de l'entreprise.

67. Les systèmes et contrôles que les établissements devraient mettre en place pour identifier les risques émergents comprennent:

- Des processus permettant de s'assurer que les informations internes sont réexaminées régulièrement afin d'identifier les tendances et les questions émergentes concernant les relations d'affaires individuelles et les activités commerciales de l'établissement.
- Des processus permettant de s'assurer que l'établissement réexamine régulièrement les sources d'information pertinentes, telles que celles visées aux points 15 et 16 des présentes orientations. Ces processus nécessitent en particulier:

  i. de réexaminer régulièrement des comptes rendus parus dans les médias concernant les secteurs ou les pays ou territoires dans lesquels opère l'établissement;

  ii. de réexaminer régulièrement les alertes et des signalements d'ordre répressif;

  iii. de veiller à ce que l'établissement prenne connaissance, dès qu'ils surviennent , des changements intervenus dans les alertes terroristes et les régimes de sanctions, par exemple en réexaminant régulièrement les alertes terroristes et en recherchant les modifications apportées aux régimes de sanctions; et

  iv. de réexaminer régulièrement des études thématiques et autres publications émanant des autorités compétentes.

- Des processus permettant de collecter et de réexaminer les informations sur les risques liés aux nouveaux produits.
- L'engagement d'un dialogue avec d'autres représentants du secteur et avec les autorités compétentes (par exemple, tables rondes, conférences et prestataires de formations), et des processus de retour d'information pour communiquer les éventuelles conclusions au personnel concerné.
- L'établissement d'une culture du partage des informations au sein de l'établissement et d'une éthique d'entreprise solide.

68. Les systèmes et contrôles que les établissements devraient mettre en place pour tenir à jour leurs évaluations de risques individuelles et à l'échelle de l'entreprise peuvent porter notamment sur les aspects suivants:

- Fixer la date à laquelle la prochaine mise à jour de l'évaluation des risques sera effectuée, par exemple le 1er mars de chaque année, pour s'assurer que les risques nouveaux ou émergents sont pris en compte dans les évaluations de risques. Lorsque l'établissement prend connaissance de l'apparition d'un nouveau risque ou de l'augmentation d'un risque existant, il devrait en rendre compte dès que possible dans les évaluations de risques.
- Enregistrer soigneusement tout au long de l'année les événements qui pourraient avoir une incidence sur les évaluations de risques, telles que les déclarations de transaction suspecte effectuées, les manquements à la conformité ou les renseignements émanent du *front office*

69. Comme pour évaluations de risques initiales, toute mise à jour d'une évaluation de risques ou toute adaptation des mesures de vigilance à l'égard de la clientèle qui l'accompagne devrait être appropriée et proportionnée au risque de BC/FT.

Systèmes et contrôles

70. Les établissements devraient prendre des mesures pour s'assurer que leurs systèmes de gestion du risque et contrôles, en particulier ceux liés à l'application du niveau adéquat de vigilance à l'égard de la clientèle, sont efficaces et proportionnés.

Conservation des documents et pièces

71. Les établissements devraient conserver et documenter les évaluations des risques liés aux relations d'affaires, ainsi que toute modification apportée à celles-ci dans le cadre des réexamens et du contrôle qu'ils effectuent, de façon à pouvoir démontrer aux autorités compétentes l'adéquation des évaluations de risques et les mesures de gestion des risques associées.

Titre III – Orientations spécifiques à certains secteurs

72. Les orientations spécifiques à certains secteurs énumérées au titre III complètent les orientations générales exposées au titre II des présentes orientations. Elles devraient être lues conjointement avec le titre II des présentes orientations.

73. Les facteurs de risque décrits dans chaque chapitre du titre III ne sont pas exhaustifs. Les établissements devraient avoir une vue globale des risques associés à la situation et garder à l'esprit que les facteurs de risque isolés ne signifient pas nécessairement qu'une relation d'affaires ou une transaction conclue à titre occasionnel doive être classée dans une catégorie de risque plus élevée ou plus faible.

74. Chaque chapitre du titre III expose également des exemples de mesures de vigilance à l'égard de la clientèle que les établissements devraient appliquer en fonction de leur appréciation des risques dans les situations à risque élevé et, dans lorsque c'est autorisé par le droit national, dans les situations à faible risque. Ces exemples ne sont pas exhaustifs, et les établissements devraient adopter les mesures de vigilance à l'égard de la clientèle les plus adaptées en fonction du niveau et du type de risque de BC/FT qu'ils ont identifié.

Chapitre 1: Orientations sectorielles pour les banques correspondantes

75. Ce chapitre fournit des orientations sur les banques correspondantes, telles que définies à l'article 3, paragraphe 8, point a), de la directive (UE) 2015/849. Les établissements offrant d'autres relations de correspondance, telles que définies à l'article 3, paragraphe 8, point b), de la directive (UE) 2015/849 devraient appliquer les présentes orientations, s'il y a lieu.

76. Dans une relation de banque correspondante, cette dernière fournit des services bancaires à un établissement client, soit pour son compte propre, soit au nom des clients de l'établissement client. L'établissement correspondant n'entretient généralement pas de relation d'affaires avec les clients de l'établissement client et ne connaît généralement pas leur identité ni la nature ou l'objet de la transaction sous-jacente, à moins que ces informations ne figurent dans l'ordre de paiement.

77. Les banques devraient prendre en considération les facteurs de risque et les mesures indiqués ci-dessous, ainsi que ceux énoncés au titre II des présentes orientations.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

78. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le compte peut être utilisé par d'autres banques clientes qui ont une relation directe avec l'établissement client mais pas avec la banque correspondante [«nesting» compte imbriqué ou encore dans le cas de compensation d'aval (*downstream clearing*)], de telle sorte que l'établissement correspondant fournit indirectement des services à d'autres banques qui ne sont pas parmi ses établissements clients.
- Le compte peut être utilisé par d'autres entités au sein du groupe de l'établissement client qui n'ont pas elles-mêmes fait l'objet de mesures de vigilance de la part de l'établissement correspondant.
- Le service comporte l'ouverture d'un compte «de passage» (*payable-through account*) qui permet aux clients de l'établissement client d'exécuter des transactions directement sur le compte de l'établissement client.

79. Les facteurs suivants peuvent contribuer à une diminution du risque:

- La relation est limitée à une capacité SWIFT RMA, qui est destinée à gérer les communications entre établissements financiers. Dans une relation SWIFT RMA, l'établissement client, ou la contrepartie, n'a pas de relation de compte de paiement.
- Plutôt que de traiter les transactions au nom de leurs clients sous-jacents, les banques agissent pour leur compte propre, par exemple dans le cas de services de bureaux de change entre deux banques, où les transactions sont conclues pour compte propre entre les banques et où le

règlement d'une transaction n'implique pas de paiement à un tiers. Dans ces hypothèses, la transaction est exécutée pour le compte de la banque cliente.

- La transaction concerne la vente, l'achat ou le nantissement de titres sur des marchés réglementés, par exemple lorsque la banque agit en tant que dépositaire ou fait appel à un dépositaire ayant un accès direct, généralement par l'intermédiaire d'un acteur local, à un système de règlement de titres de l'Union européenne ou autre.

Facteurs de risque liés aux clients

80. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Les politiques de l'établissement client en matière de lutte contre le BC/FT et les systèmes et contrôles mis en place par l'établissement client pour les mettre en œuvre ne répondent pas aux normes requises par la directive (UE) 2015/849.
- L'établissement client n'est pas soumis à une surveillance adéquate en matière de lutte contre le BC/FT.
- L'établissement client, sa société mère ou une entreprise appartenant au même groupe que l'établissement client a récemment fait l'objet de mesures d'application de la réglementation du fait de l'inadéquation de ses politiques et procédures en matière de lutte contre le BC/FT et/ou d'infractions aux obligations de lutte contre le BC/FT.
- L'établissement client exécute des transactions commerciales significatives avec des secteurs qui sont associés à des niveaux de risque plus élevés de BC/FT; par exemple, l'établissement client effectue des opérations de transmission de fonds ou des transactions de montant significatif, au nom de certaines sociétés de transmission de fonds ou de certains bureaux de change, avec des non-résidents ou dans une devise autre que celle du pays dans lequel il est installé.
- Parmi les dirigeants ou propriétaires de l'établissement client figurent des PPE, en particulier lorsqu'une PPE peut exercer une influence significative sur l'établissement client, lorsque la réputation, l'intégrité ou l'aptitude de la PPE en tant que membre du conseil d'administration ou personne exerçant des fonctions clés est une source d'inquiétude, ou lorsque la PPE est issue d'un pays ou territoire associé à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ou territoires où la corruption est perçue comme systémique ou généralisée.
- L'historique de la relation d'affaires avec l'établissement client suscite des inquiétudes, par exemple lorsque le montant des transactions ne correspond pas à celui auquel l'établissement correspondant s'attendrait au regard de sa connaissance de la nature et de la taille de l'établissement client.

81. Les facteurs suivants peuvent contribuer à une diminution du risque, lorsque l'établissement correspondant s'est assuré que:

- les contrôles effectués par l'établissement client en matière de lutte contre le BC/FT sont au moins équivalents à ceux requis par la directive (UE) 2015/849;
- l'établissement client qui fait partie du même groupe que l'établissement correspondant, n'est pas établi dans un pays ou territoire associé à un risque plus élevé de BC/FT, et respecte efficacement des normes en matière de lutte contre le blanchiment de capitaux à l'échelle du groupe qui ne sont pas moins strictes que celles requises par la directive (UE) 2015/849.

Facteurs de risque liés aux pays ou zones géographiques

82. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- L'établissement client est installé dans un pays ou territoire associé à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ou territoires
    - présentant des niveaux significatifs de corruption et/ou autres infractions sous-jacentes au blanchiment de capitaux;
    - dont le système juridique et judiciaire ne dispose pas de la capacité adéquate pour poursuivre efficacement ces infractions; ou
    - n'assurant pas une supervision efficace en matière de lutte contre le BC/FT[18].
- L'établissement client exécute des transactions commerciales significatives avec des clients installés dans un pays ou territoire associé à un risque plus élevé de BC/FT.
- L'entreprise mère de l'établissement client a son siège ou est établie dans un pays ou territoire associé à un risque plus élevé de BC/FT.

83. Les facteurs suivants peuvent contribuer à une diminution du risque:

- L'établissement client est installé dans un pays membre de l'EEE.
- L'établissement client est installé dans un pays tiers dont les exigences de lutte contre le BC/FT sont au moins équivalentes à celles requises par la directive (UE) 2015/849 et qui assure la mise en œuvre effective de ces exigences (les correspondantes devraient toutefois noter que cela ne les exonère pas de l'obligation d'appliquer les mesures de vigilance renforcées à l'égard de la clientèle visées à l'article 19 de la directive (UE) 2015/849).

Mesures

84. Tous les établissements correspondants doivent prendre des mesures de vigilance à l'égard de l'établissement client, qui est leur client, en fonction de leur appréciation des risques.[19]

    Par conséquent, les établissements correspondants doivent:

[18] Voir également titre II, points 22 à 27.

[19] Article 13 de la directive (UE) 2015/849.

- Identifier et vérifier l'identité de l'établissement client et de son bénéficiaire effectif. Dans ce contexte, les établissements correspondants devraient obtenir suffisamment d'informations sur les activités et la réputation de l'établissement client afin de s'assurer que le risque de blanchiment de capitaux associé à l'établissement client n'est pas plus élevé.

    i. Les établissements correspondants devraient notamment obtenir des informations sur les dirigeants de l'établissement client et examiner la pertinence, à des fins de prévention de la criminalité financière, des éventuels liens que les dirigeants ou propriétaires de l'établissement client pourraient avoir avec des PPE ou avec d'autres individus à haut risque;

    ii. et considérer, en fonction d'une appréciation des risques, l'opportunité ou non d'obtenir des informations sur les principales activités commerciales de l'établissement client, sur les types de clients qu'il attire et sur la qualité de ses systèmes et contrôles en matière de lutte contre le blanchiment de capitaux (y compris des informations accessibles au public concernant d'éventuelles sanctions réglementaires ou pénales en cas de manquements aux obligations de lutte contre le blanchiment de capitaux). Lorsque l'établissement client est une filiale, une succursale ou un établissement affilié, les correspondants devraient également prendre en considération le statut, la réputation et les contrôles mis en place par l'entreprise mère pour lutter contre le blanchiment de capitaux.

- Établir et documenter la nature et l'objet du service fourni, ainsi que les responsabilités de chaque établissement. Cela pourrait comprendre l'établissement, par écrit, de l'étendue de la relation, des produits et services qui seront fournis, des modalités d'utilisation du service de correspondance bancaire, et par qui ce service peut être utilisé (en indiquant, par exemple, s'il peut être utilisé par d'autres banques dans le cadre de leur relation avec l'établissement client).

- Contrôler la relation d'affaires, y compris les transactions, pour identifier les changements intervenus dans le profil de risque de l'établissement client et pour détecter tout comportement inhabituel ou suspect, y compris les activités qui ne sont pas compatibles avec l'objet des services fournis ou qui sont contraires aux engagements conclus entre le correspondant et l'établissement client. Lorsque la banque correspondante donne aux clients de l'établissement client un accès direct aux comptes [par exemple des comptes de passage ou des comptes «imbriqués» (*nested accounts*)], elle devrait assurer un contrôle renforcé de la relation d'affaires sur une base continue. En raison de la nature des services de banque de correspondance, le contrôle post-exécution est la norme.

- Veiller à ce que les informations dont ils disposent concernant les mesures de vigilance à l'égard de la clientèle soient à jour.

85. Les établissements correspondants doivent également s'assurer que l'établissement client n'autorise pas l'utilisation de ses comptes par une banque écran,[20] conformément à l'article 24 de la directive (UE) 2015/849. Les établissements correspondants pourraient notamment

[20] Article 3, paragraphe 17, de la directive (UE) 2015/849.

demander à l'établissement client de confirmer qu'il ne traite pas avec des banques fictives, recenser les éléments pertinents des politiques et procédures de l'établissement client, ou prendre en considération les informations accessibles au public, telles que les dispositions légales interdisant la fourniture de services à des banques fictives.

86. En ce qui concerne les relations transfrontalières de correspondance avec des établissements clients de pays tiers, l'article 19 de la directive (UE) 2015/849 requiert que, outre les mesures de vigilance à l'égard de la clientèle visées à l'article 13 de la directive (UE) 2015/849, l'établissement correspondant applique des mesures de vigilance renforcées spécifiques à l'égard de la clientèle.

87. La directive (UE) 2015/849 n'oblige pas les établissements correspondants à appliquer des mesures de vigilance à l'égard des clients individuels de l'établissement client.

88. Les établissements correspondants devraient garder à l'esprit que les questionnaires de vigilance à l'égard de la clientèle fournis par des organisations internationales ne sont généralement pas conçus pour aider spécifiquement les établissements correspondants à respecter leurs obligations au titre de la directive (UE) 2015/849. Lorsqu'ils s'interrogent sur l'opportunité d'utiliser ces questionnaires, les établissements correspondants devraient apprécier si ceux-ci seront suffisants pour leur permettre de respecter leurs obligations au titre de la directive (UE) 2015/849 et devraient prendre, si nécessaire, des mesures supplémentaires.

Établissements clients installés dans des pays non membres de l'EEE

89. Lorsque l'établissement client est installé dans un pays tiers, l'article 19 de la directive (UE) 2015/849 exige que, outre les mesures de vigilance à l'égard de la clientèle visées à l'article 13 de la directive (UE) 2015/849, les établissements correspondants appliquent des mesures de vigilance renforcées spécifiques à l'égard de la clientèle.

90. Les établissements correspondants doivent appliquer chacune de ces mesures de vigilance renforcées à l'égard des établissements clients installés dans un pays non membre de l'EEE, mais les correspondants peuvent adapter l'étendue de ces mesures en fonction de leur appréciation des risques. Par exemple, si l'établissement correspondant s'est assuré, sur la base de recherches adéquates, que l'établissement client est installé dans un pays tiers disposant d'un dispositif efficace de lutte contre le blanchiment de capitaux et le financement du terrorisme, qu'il fait l'objet d'une surveillance efficace en ce qui concerne le respect de ces exigences, et qu'il n'existe pas de raisons de soupçonner que les politiques et procédures de l'établissement client en matière de lutte contre le blanchiment de capitaux sont inadéquates ou ont récemment été jugées inadéquates, il peut ne pas être nécessaire de procéder à une évaluation détaillée des contrôles mis en place par l'établissement client pour lutter contre le blanchiment de capitaux.

91. Les établissements correspondants devraient toujours documenter de manière adéquate les mesures de vigilance et les mesures de vigilance renforcées qu'ils prennent à l'égard de la clientèle, ainsi que leurs processus de prise de décision.

92. L'article 19 de la directive (UE) 2015/849 exige des établissements correspondants qu'ils prennent des mesures fondées sur l'appréciation des risques pour:

- recueillir des informations suffisantes sur l'établissement client pour comprendre pleinement la nature de ses activités commerciales et pour établir dans quelle mesure ces activités exposent le correspondant à un risque de blanchiment de capitaux plus élevé. Il y aurait lieu de notamment mettre en œuvre des mesures visant à comprendre et à évaluer les risques liés à la nature de la clientèle de l'établissement client et le type de transactions que celui-ci exécutera par le biais du compte de correspondance.
- Déterminer, sur la base d'informations accessibles au public, la réputation de l'établissement client et la qualité de la surveillance. Cela signifie que l'établissement correspondant devrait apprécier dans quelle mesure il peut se satisfaire du fait que l'établissement client fait l'objet d'une surveillance adéquate en ce qui concerne le respect de ses obligations de lutte contre le blanchiment de capitaux. Plusieurs ressources accessibles au public, comme les évaluations du GAFI ou du FSAP, qui comprennent des rubriques sur la surveillance efficace, peuvent aider les établissements correspondants à procéder à cette appréciation.
- Évaluer les contrôles mis en place par l'établissement client pour lutter contre le blanchiment de capitaux et le financement du terrorisme. Cela signifie que l'établissement correspondant devrait procéder à une évaluation qualitative du dispositif de contrôle de l'établissement client en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, et ne pas se contenter d'obtenir une copie des politiques et procédures de l'établissement client en matière de lutte contre le blanchiment de capitaux. Cette évaluation devrait être documentée de manière adéquate. Conformément à l'approche fondée sur les risques, lorsque le risque est particulièrement élevé, et en particulier lorsque le volume de transactions bancaires de l'établissement correspondant est important, l'établissement correspondant devrait envisager la réalisation d'inspections sur place et/ou l'analyse par sondage pour s'assurer que les politiques et procédures de l'établissement client en matière de lutte contre le blanchiment de capitaux sont mises en œuvre efficacement.
- Obtenir l'autorisation d'un membre d'un niveau élevé de la hiérarchie, tel que défini à l'article 3, paragraphe 12, de la directive (UE) 2015/849, avant de nouer de nouvelles relations de correspondance. Le membre d'un niveau élevé de la hiérarchie qui donne l'autorisation ne devrait pas être le dirigeant qui parraine la relation, et plus le risque associé à la relation est élevé, plus le dirigeant devrait occuper une position élevée dans la hiérarchie. Les établissements correspondants devraient tenir les dirigeants informés des relations bancaires de correspondance à haut risque ainsi que des mesures prises à leur niveaupour gérer ce risque efficacement.
- Documenter les responsabilités de chaque établissement. Cette obligation pourrait faire partie des conditions générales standards de l'établissement correspondant, mais les établissements

correspondants devraient établir par écrit les modalités d'utilisation du service bancaire de correspondance, en indiquant par qui ce service peut être utilisé (par exemple, s'il peut être utilisé par d'autres banques dans le cadre de leur relation avec l'établissement client), ainsi que les responsabilités de l'établissement client en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Lorsque le risque associé à la relation est élevé, il peut être utile que l'établissement correspondant s'assure que l'établissement client respecte ses responsabilités au titre de cet accord, par exemple à l'aide d'un contrôle ex post des transactions.

- En ce qui concerne les comptes de passage et les comptes imbriqués, s'assurer que l'établissement de crédit ou l'établissement financier client a vérifié l'identité du client ayant un accès direct aux comptes de l'établissement correspondant et a exercé à son égard une vigilance constante, et qu'il peut fournir des données pertinentes concernant ces mesures de vigilance à la demande de l'établissement correspondant. Les établissements correspondants devraient s'efforcer d'obtenir de l'établissement client la confirmation que les données pertinentes peuvent être fournies sur demande.

Établissements clients installés dans des pays de l'EEE

93. Lorsque l'établissement client est installé dans un pays de l'EEE, l'article 19 de la directive (UE) 2015/849 n'est pas applicable. Toutefois, l'établissement correspondant demeure tenu d'appliquer des mesures de vigilance à l'égard de la clientèle fondées sur l'appréciation des risques, en application de l'article 13 de la directive (UE) 2015/849.

94. Lorsque le risque associé à un établissement client installé dans un État membre de l'EEE est accru, les établissements correspondants doivent appliquer des mesures de vigilance renforcées à l'égard de la clientèle conformément à l'article 18 de la directive (UE) 2015/849. Dans ce cas, les établissements correspondants devraient envisager d'appliquer au moins certaines des mesures de vigilance renforcées à l'égard de la clientèle visées à l'article 19 de la directive (UE) 2015/849, en particulier à l'article 19, points a) et b).

Chapitre 2: Orientations sectorielles pour les banques de détail

95. Aux fins des présentes orientations, il faut entendre par banque de détail la fourniture de services bancaires aux personnes physiques et aux petites et moyennes entreprises. Les produits et services de banque de détail comprennent les comptes courants, les crédits immobiliers, les comptes d'épargne, les crédits à la consommation et les prêts à terme («term loans»), ainsi que les lignes de crédit.

96. En raison de la nature des produits et services proposés, de la relative facilité d'accès et du volume de transactions et de relations d'affaires souvent important, la banque de détail est vulnérable au financement du terrorisme et à toutes les étapes du processus de blanchiment de capitaux. Dans le même temps, le volume de relations d'affaires et de transactions associées à la banque de détail peut rendre particulièrement difficiles l'identification du risque de BC/FT associé aux différentes relations ainsi que la détection des transactions suspectes.

97. Les banques devraient prendre en considération les facteurs de risque et les mesures indiqués ci-dessous, ainsi que ceux énoncés au titre II des présentes orientations.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

98. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- les caractéristiques du produit favorisent l'anonymat;
- le produit permet des paiements de tiers qui ne sont ni associés au produit, ni identifiés à l'avance, lorsque de tels paiements ne sont pas normalement prévus, par exemple pour des crédits immobiliers ou des prêts;
- le produit ne fixe aucune limitation quant au chiffre d'affaires, aux transactions transfrontalières et autres caractéristiques du produit;
- les nouveaux produits et les nouvelles pratiques commerciales, notamment les nouveaux mécanismes de distribution, et l'utilisation de technologies nouvelles ou en cours de développement pour des produits nouveaux et existants lorsque ceux-ci ne sont pas encore bien compris;
- les prêts (y compris les crédits immobiliers) garantis par la valeur de biens situés dans d'autres pays ou territoires, en particulier les pays ou territoires où il est difficile de déterminer si le client est le propriétaire légitime de la garantie, ou lorsque l'identité des parties garantissant le prêt est difficile à vérifier;
- un volume ou un montant de transactions inhabituellement élevé.

99. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Le produit dispose de fonctionnalités limitées, par exemple dans le cas:

i. d'un produit d'épargne à durée déterminée assorti de faibles seuils d'épargne;

ii. d'un produit dont les prestations ne peuvent pas être réalisées au profit d'un tiers;

iii. d'un produit dont les prestations ne sont réalisables qu'à long terme ou pour une finalité spécifique, telle que la retraite ou l'achat d'un bien immobilier;

iv. d'une facilité de crédit d'un faible montant, y compris un crédit subordonné à l'achat d'un bien de consommation ou d'un service donné; ou

v. d'un produit de faible valeur, y compris un bail, lorsque la propriété légale et effective du bien n'est transférée au client qu'après la fin de la relation contractuelle ou n'est jamais cédée.

- Le produit ne peut être détenu que par certaines catégories de clients, par exemple des retraités, des parents au nom de leurs enfants, ou des mineurs jusqu'à ce qu'ils atteignent l'âge de la majorité.
- Les transactions doivent être effectuées par le biais d'un compte détenu au nom du client auprès d'un établissement de crédit ou d'un établissement financier qui est soumis à des exigences de lutte contre le BC/FT qui sont au moins équivalentes à celles requises par la directive (UE) 2015/849.
- Il n'existe pas de possibilité de paiement excédentaire (*overpayment facility*).

Facteurs de risque liés aux clients

100. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- La nature du client, par exemple:

i. Le client est une entreprise nécessitant beaucoup d'espèces.

ii. Le client est une entreprise associée à un niveau de risque de blanchiment de capitaux plus élevé, par exemple certaines entreprises de transmission de fonds ou certains prestataires de services de jeux d'argent et de hasard.

iii. Le client est une entreprise associée à un risque de corruption plus élevé, par exemples les entreprises spécialisées dans les activités extractives ou le commerce des armes.

iv. Le client est un organisme à but non lucratif qui soutient des pays ou territoires associés à un risque de financement du terrorisme accru.

v. Le client est une nouvelle entreprise dont le profil ou le bilan commercial n'est pas adéquat.

vi. Le client est un non résident. Les banques devraient noter que l'article 16 de la directive 2014/92/EU instaure le droit pour les consommateurs résidant légalement dans l'Union

européenne d'obtenir un compte bancaire de base, bien que le droit d'ouvrir et d'utiliser un compte de paiement de base s'applique uniquement dans la mesure où les banques peuvent respecter leurs obligations de lutte contre le BC/FT et n'exonère pas les banques de leur obligation d'identifier et d'évaluer le risque de blanchiment de capitaux et de financement du terrorisme, y compris le risque lié au fait que le client ne soit pas résident de l'État membre dans lequel la banque est installée[21].

vii. Le bénéficiaire effectif du client ne peut être identifié facilement, par exemple parce que la structure de propriété du client est inhabituelle, anormalement complexe ou opaque, ou parce que le client émet des actions au porteur.

- Le comportement du client, par exemple:

  i. Le client est peu enclin à fournir des informations sur les mesures de vigilance à l'égard de la clientèle ou semble éviter délibérément tout contact en face à face.

Le justificatif d'identité du client est présenté sous une forme inhabituelle sans raison apparente.
Le comportement ou le volume de transactions du client ne correspond pas à celui attendu dans la catégorie à laquelle il appartient ou est inhabituel au regard des informations fournies par le client lors de l'ouverture du compte.
Le comportement du client est inhabituel, par exemple le client accélère, de manière inattendue et sans explication raisonnable, l'échéancier de remboursement convenu, soit par des remboursements forfaitaires, soit par résiliation anticipée; dépose ou demande, sans raison apparente, le paiement de billets de banque d'un montant élevé; augmente son activité après une période d'inactivité; ou effectue des transactions qui semblent ne répondre à aucune logique économique.

101. Le facteur suivant peut contribuer à une diminution du risque:

- Le client est un client de longue date dont les précédentes transactions n'ont pas fait naître de soupçons ou d'inquiétudes, et le produit ou service demandé est conforme au profil de risque du client.

Facteurs de risque liés aux pays ou zones géographiques[22]

102. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Les fonds du client proviennent de liens personnels ou commerciaux avec des pays ou territoires associés à un risque plus élevé de BC/FT.
- Le bénéficiaire est installé dans un pays ou territoire associé à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ou territoires connus pour financer ou soutenir des activités terroristes ou dans lesquels opèrent des groupes connus pour commettre des infractions terroristes, ainsi qu'aux pays ou territoires soumis à des

[21] Voir l'«Avis sur l'application de mesures de vigilance à l'égard de clients qui sont des demandeurs d'asile issus de pays ou de territoires tiers à haut risque» de l'ABE: http://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+client+Due+Diligence+on+Asylum+Seekers%29.pdf

[22] Voir également le titre II.

sanctions financières, à des embargos ou à des mesures liées au terrorisme, au financement du terrorisme ou à la prolifération.

103. Le facteur suivant peut contribuer à une diminution du risque:

- Les pays associés à la transaction disposent d'un dispositif de lutte contre le BC/FT qui n'est pas moins solide que celui requis en application de la directive (UE) 2015/849 et sont associés à des niveaux d'infractions sous-jacentes faibles.

Facteurs de risque liés aux canaux de distribution

104. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- les relations d'affaires n'impliquant pas la présence physique des parties, lorsque des garanties adéquates supplémentaires – par exemple une signature électronique, des certificats d'identification électronique émis conformément au règlement (UE) nº 910/2014 ou des vérifications pour lutter contre la fraude liée à l'usurpation d'identité – n'ont pas été mises en place;
- s'appuyer sur les mesures de vigilance prises par un tiers à l'égard de la clientèle dans les situations où la banque n'entretient pas de relation de longue date avec le tiers référent;
- les nouveaux canaux de distribution n'ont pas encore été testés.

105. Le facteur suivant peut contribuer à une diminution du risque:

- Le produit n'est disponible que pour les clients qui répondent à des critères d'admissibilité spécifiques fixés par les autorités publiques nationales, comme dans le cas des bénéficiaires d'allocations publiques ou de certains produits d'épargne pour enfants déclarés dans un État membre donné.

Mesures

106. Lorsque les banques utilisent des systèmes automatisés pour identifier le risque de BC/FT associé aux relations d'affaires individuelles ou aux transactions conclues à titre occasionnel et pour identifier les transactions suspectes, elles devraient veiller à ce que ces systèmes soient adaptés à l'usage prévu conformément aux critères énoncés au titre II. L'utilisation de systèmes informatiques automatisés ne devrait jamais être considérée comme se substituant à la vigilance du personnel.

Mesures de vigilance renforcées à l'égard de la clientèle

107. Lorsque le risque associé à une relation d'affaires ou à une transaction conclue à titre occasionnel est accru, les banques doivent appliquer des mesures de vigilance renforcées à l'égard de la clientèle[23]. Ces mesures peuvent comprendre:

[23] Article 18 de la directive (UE) 2015/849.

- Vérifier l'identité du client et du bénéficiaire effectif sur la base de plusieurs sources fiables et indépendantes.
- Identifier et vérifier l'identité d'autres actionnaires qui ne sont pas le bénéficiaire effectif du client ou de toute personne physique autorisée à gérer un compte ou à donner des ordres concernant le transfert de fonds ou de titres.
- Obtenir plus d'informations sur le client et sur la nature ou l'objet de la relation d'affaires afin de construire un profil de client plus complet, par exemple en effectuant des recherches de mentions négatives dans les médias ou des recherches en sources ouvertes, ou en commandant un rapport de renseignement auprès d'un tiers. Le type d'informations que les banques peuvent rechercher peut inclure:

    i. la nature des activités ou de la profession du client;

    ii. l'origine du patrimoine du client et l'origine des fonds du client qui sont impliqués dans la relation d'affaires, afin d'obtenir l'assurance raisonnable que ceux-ci sont légitimes;

    iii. l'objet de la transaction, y compris, le cas échéant, la destination des fonds du client;

    iv. des informations sur les éventuels liens que le client pourrait entretenir avec d'autres pays ou territoires (sièges, sites opérationnels, filiales, etc.) et sur les personnes susceptibles d'influencer ses activités; ou

    v. lorsque le client est installé dans un autre pays, les raisons pour lesquelles il demande des services de banque de détail en dehors de son pays ou territoire de résidence.

- Augmenter la fréquence du contrôle des transactions.
- Réexaminer et, si nécessaire, mettre à jour les informations et les documents détenus plus fréquemment. Lorsque le risque associé à la relation est particulièrement élevé, les banques devraient réexaminer la relation d'affaires chaque année.

Mesures de vigilance simplifiées à l'égard de la clientèle

108. Dans les situations à faible risque, et dans la mesure où cela est autorisé par le droit national, les banques peuvent appliquer des mesures simplifiées de vigilance à l'égard de la clientèle qui peuvent comprendre:

- pour les clients qui font l'objet d'un régime d'inscription ou d'autorisation obligatoire, la vérification de l'identité sur la base de preuves attestant que le client est soumis à ce régime, par exemple en effectuant une recherche dans le registre public du régulateur;
- la vérification de l'identité du client et, le cas échéant, du bénéficiaire effectif pendant l'établissement de la relation d'affaires, conformément à l'article 14, paragraphe 2, de la directive (UE) 2015/849;

- la présomption qu'un paiement débité d'un compte détenu au nom du client, à titre individuel ou joint, auprès d'un établissement de crédit ou d'un établissement financier réglementé dans un pays de l'EEE remplit les exigences prévues à l'article 13, paragraphe 1, points a) et b), de la directive (UE) 2015/849;
- l'acceptation d'autres formes d'identité répondant au critère de source indépendante et fiable visé à l'article 13, paragraphe 1, point a), de la directive (UE) 2015/849, telles qu'une lettre adressée au client par un organisme gouvernemental ou autre organe public fiable, lorsque le client n'est pas en mesure, pour des motifs raisonnables avérés, de fournir les justificatifs d'identité habituels, et pour autant qu'il n'y ait pas de motif de suspicion;
- la mise à jour des informations relatives aux mesures de vigilance à l'égard de la clientèle uniquement dans le cas de certains évènements déclencheurs, par exemple si le client demande un produit nouveau ou plus risqué, ou en cas de changements dans le comportement ou le profil de transaction du client qui semblent indiquer que le risque associé à la relation n'est plus faible.

Compte communs

109. Lorsque le client d'une banque ouvre un «compte commun» (*pooled account*) afin d'administrer les fonds appartenant à ses propres clients, la banque devrait appliquer toutes les mesures de vigilance nécessaires, y compris traiter les clients du client comme les bénéficiaires effectifs des fonds détenus sur le compte commun et vérifier leur identité.

110. Lorsqu'il existe des indices selon lesquels le risque associé à la relation d'affaires est élevé, les banques doivent appliquer des mesures de vigilance renforcées à l'égard de la clientèle, s'il y a lieu[24].

111. Toutefois, dans la mesure où cela est autorisé par le droit national, lorsque le risque associé à la relation d'affaires est faible et sous réserve des conditions exposées ci-dessous, une banque peut appliquer des mesures de vigilance simplifiées à l'égard de la clientèle à condition que:

- le client soit un établissement soumis à des obligations de lutte contre le BC/FT dans un État membre de l'EEE ou dans un pays tiers dont le dispositif de lutte contre le BC/FT n'est pas moins solide que celui requis par la directive (UE) 2015/849 et qui fait l'objet d'une surveillance efficace en ce qui concerne le respect de ces exigences;
- le client ne soit pas un établissement mais une autre entité assujettie qui est soumise à des obligations de lutte contre le BC/FT dans un État membre de l'EEE et qui fait l'objet d'une surveillance efficace en ce qui concerne le respect de ces exigences;
- le risque de BC/FT associé à la relation d'affaires soit faible, compte tenu de l'évaluation par la banque des activités commerciales de son client, des types de clients servis par l'entreprise du client et des pays ou territoires auxquels sont exposées les activités du client, entre autres considérations;

[24] Articles 13, paragraphe 1, et 18, paragraphe 1, de la directive (UE) 2015/849.

- la banque se soit assurée que le client applique des mesures de vigilance solides et fondées sur l'appréciation des risques à l'égard de ses propres clients et des bénéficiaires effectifs de ses clients (il peut être utile pour la banque de prendre des mesures fondées sur l'appréciation des risques afin d'évaluer l'adéquation des politiques et procédures mises en place par son client en matière de vigilance à l'égard de la clientèle, par exemple en assurant la liaison directe avec le client); et
- que la banque ait pris des mesures fondées sur l'appréciation des risques afin de s'assurer que le client fournira immédiatement sur demande des informations et des documents concernant les mesures de vigilance prises à l'égard de ses clients sous-jacents qui sont les bénéficiaires effectifs des fonds détenus sur le compte commun, par exemple en incorporant des dispositions adéquates dans un contrat avec le client ou en analysant par sondage la capacité du client à fournir sur demande des informations sur les mesures de vigilance à l'égard de la clientèle.

112. Lorsque les conditions d'application de mesures de vigilance simplifiées aux comptes communs [pooled account] sont réunies, la banque peut notamment prendre les mesures de vigilance simplifiées suivantes à l'égard de la clientèle:

- l'identification et la vérification de l'identité du client, y compris des bénéficiaires effectifs du client (mais pas des clients sous-jacents du client);
- l'analyse de l'objet et de la nature envisagée de la relation d'affaires; et
- la réalisation d'un contrôle continu de la relation d'affaires.

Chapitre 3: Orientations sectorielles pour les émetteurs de monnaie électronique

113. Ce chapitre fournit des orientations pour les émetteurs de monnaie électronique tels que définis à l'article 2, paragraphe 3, de la directive 2009/110/CE. Le niveau de risque de BC/FT associé à la monnaie électronique[25] dépend principalement des caractéristiques des différents produits de monnaie électronique et de la mesure dans laquelle les émetteurs de monnaie électronique ont recours à d'autres personnes agissant pour leur compte pour distribuer et rembourser de la monnaie électronique[26].

114. Les établissements qui émettent de la monnaie électronique devraient prendre en considération les mesures et les facteurs de risque exposés ci-après, ainsi que ceux visés au titre II des présentes orientations. Les orientations sectorielles pour les entreprises de transmission de fonds énoncées au titre III, chapitre 4, pourraient également être pertinentes dans ce contexte.

Facteurs de risque

Facteurs de risque liés aux produits

115. Les émetteurs de monnaie électronique devraient prendre en compte le risque de BC/FT lié:

- aux seuils;
- aux modalités de chargement; et
- à la fonctionnalité et la négociabilité.

116. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Seuils: le produit permet

  i. les paiements, le chargement ou le remboursement, y compris le retrait d'espèces d'un montant élevé ou illimité;

  ii. les paiements, le chargement ou le remboursement, y compris le retrait d'espèces d'un montant élevé;

  iii. le stockage de fonds d'un montant élevé ou illimité sur le produit/compte de monnaie électronique.

[25] Article 2, paragraphe 2, de la directive 2009/110/CE.

[26] Article 3, paragraphe 4, de la directive 2009/110/CE.

- Modalités de chargement: le produit peut être

  i. chargé de manière anonyme, par exemple au moyen d'espèces, de monnaie électronique anonyme ou de produits de monnaie électronique bénéficiant de l'exemption visée à l'article 12 de la directive (UE) 2015/849;

  ii. crédité au moyen de paiements de tiers non identifiés;

  iii. crédité au moyen d'autres produits de monnaie électronique.

- Fonctionnalités et négociabilité: le produit

  i. permet les virements entre personnes;

  ii. est accepté comme mode de règlement par un grand nombre de commerçants et de points de vente;

  iii. est conçu spécialement pour être accepté comme mode de règlement par des commerçants négociant des produits ou des services associés à un risque de criminalité financière élevé, par exemple les jeux d'argent et de hasard en ligne;

  iv. peut être utilisé dans des transactions transfrontalières ou dans différents pays ou territoires;

  v. est conçu pour être utilisé par des personnes autres que le client, par exemple certains produits de carte partenaire «partner card product» (à l'exception des cartes cadeaux de faible valeur);

  vi. permet les retraits d'espèces d'un montant élevé.

117. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Seuils: le produit

  i. fixe des limites d'un montant faible sur les paiements, le chargement ou le remboursement, y compris le retrait d'espèces (les établissements devraient toutefois noter qu'un seuil faible peut, seul, ne pas être suffisant pour diminuer le risque de financement du terrorisme);

  ii. limite le nombre de paiements, le chargement ou le remboursement, y compris le retrait d'espèces sur une période donnée;

  iii. limite le montant des fonds qui peuvent être stockés sur le produit/compte de monnaie électronique à un moment donné.

- Chargement:le produit

i. exige que les fonds crédités pour l'achat ou le rechargement soient débités de manière vérifiable d'un compte détenu au nom du client, à titre individuel ou joint, auprès d'un établissement de crédit ou d'un établissement financier de l'EEE;

- Fonctionnalités et négociabilité: le produit

i. ne permet pas ou limite de manière stricte le retrait d'espèces;

ii. ne peut être utilisé qu'au niveau national;

iii. est accepté par un nombre limité de commerçants ou de points de vente dont les activités sont connues de l'émetteur de monnaie électronique;

iv. est spécialement conçu pour limiter leur usage par des commerçants négociant des produits ou des services associés à un risque de criminalité financière élevé;

v. est accepté comme mode de règlement pour des catégories limitées de services ou de produits présentant un faible risque.

Facteurs de risque liés aux clients

118. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le client achète plusieurs produits de monnaie électronique auprès du même émetteur, recharge fréquemment le produit ou effectue plusieurs retraits d'espèces sur une courte durée et sans logique économique; lorsque les distributeurs (ou les agents agissant en tant que distributeurs) sont eux-mêmes des entités assujetties, cela concerne également les produits de monnaie électronique de différents émetteurs achetés auprès d'un même distributeur.
- Les transactions du client sont toujours juste en-dessous des éventuelles limites de montants/transactions.
- Le produit semble avoir été utilisé par plusieurs personnes dont l'identité n'est pas connue de l'émetteur (par exemple le produit est utilisé à partir de plusieurs adresses IP en même temps).
- Les données d'identification du client telles que l'adresse personnelle ou l'adresse IP, ou les comptes bancaires liés, sont fréquemment modifiées.
- Le produit n'est pas utilisé aux fins pour lesquelles il a été conçu, par exemple il est utilisé à l'étranger alors qu'il s'agit d'une carte cadeau d'un centre commercial.

119. Le facteur suivant peut contribuer à une diminution du risque:

- Le produit n'est accessible que pour certaines catégories de clients, par exemple les bénéficiaires de prestations sociales ou les membres du personnel d'une entreprise qui émet ces produits pour couvrir des frais professionnels.

Facteurs de risque liés aux canaux de distribution

120. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Distribution en ligne et à distance sans garanties adéquates, telles qu'une signature électronique, des documents d'identification électronique répondant aux critères prévus par le règlement (UE) nº 910/2014 ou des mesures de lutte contre la fraude liée à l'usurpation d'identité.
- Distribution par le biais d'intermédiaires qui ne sont pas eux-mêmes des entités assujetties au titre de la directive (UE) 2015/849 ou du droit national, le cas échéant, lorsque l'émetteur de monnaie électronique:

  i. a recours à l'intermédiaire pour exécuter certaines des obligations de l'émetteur de monnaie électronique en matière de lutte contre le BC/FT; et

  ii. ne s'est pas assuré que l'intermédiaire a mis en place des systèmes et contrôles adéquats en matière de lutte contre le BC/FT.

- Segmentation des services, c'est-à-dire la fourniture de services de monnaie électronique par des prestataires de services opérationnellement indépendants sans une surveillance et une coordination adéquates.

Facteurs de risque liés aux pays ou zones géographiques[27]

121. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le bénéficiaire est établi dans un pays ou territoire associé à un risque plus élevé de BC/FT, ou le produit reçoit des fonds provenant de sources établies dans de tels pays ou territoires. Les établissements devraient accorder une attention particulière aux pays ou territoires connus pour financer ou soutenir des activités terroristes ou dans lesquels opèrent des groupes connus pour commettre des infractions terroristes, ainsi qu'aux pays ou territoires soumis à des sanctions financières, à des embargos ou à des mesures liées au terrorisme, au financement du terrorisme ou à la prolifération.

Mesures

122. Le droit national peut prévoir une exemption de l'obligation d'identifier et de vérifier l'identité du client et des bénéficiaires effectifs, ainsi que de l'obligation d'évaluer la nature et l'objet de la relation d'affaires pour certains produits de monnaie électronique, conformément à l'article 12 de la directive (UE) 2015/849.

123. Les établissements devraient noter que l'exemption visée à l'article 12 de la directive (UE) 2015/849 ne s'étend pas à l'obligation d'exercer un contrôle continu des transactions et de la relation d'affaires, pas plus qu'elle ne les exonère de l'obligation d'identifier et de déclarer les

[27] Voir titre II, points 22 à 27.

transactions suspectes; cela signifie que les établissements devraient veiller à obtenir suffisamment d'informations sur leurs clients, ou sur les types de clients ciblés par leur produit, afin d'être en mesure d'exercer un contrôle continu efficace de la relation d'affaires.

124. Les types de systèmes de contrôle que les établissements devraient mettre en place comprennent notamment:

- des systèmes de contrôle des transactions qui détectent les anomalies ou les types de comportements suspects, y compris l'utilisation inattendue du produit à des fins autres que celles pour lesquelles il a été conçu; l'établissement pourrait désactiver le produit soit manuellement, soit à distance à l'aide de contrôles sur puce (*on-chip controls*) jusqu'à ce qu'il ait pu obtenir l'assurance qu'il n'y a pas de motif de suspicion;
- des systèmes qui identifient les écarts entre les informations soumises et les informations détectées, par exemple entre les informations soumises sur le pays d'origine et l'adresse IP détectée par voie électronique;
- des systèmes qui comparent les données soumises avec les données détenues sur d'autres relations d'affaires et qui peuvent identifier des constantes, par exemple le même instrument de financement ou les mêmes coordonnées de contact;
- des systèmes qui identifient si le produit est utilisé avec des commerçants négociant des produits ou des services qui sont associés à un risque de criminalité financière élevé.

Mesures de vigilance renforcées à l'égard de la clientèle

125. Les mesures de vigilance renforcées à l'égard de la clientèle que les établissements devraient appliquer dans une situation à risque élevé comprennent notamment:

- l'obtention d'informations supplémentaires sur le client lors de l'identification, comme l'origine des fonds;
- l'application de mesures de vérification supplémentaires à partir d'une plus grande variété de sources fiables et indépendantes (par exemple par croisement avec des bases de données en ligne) afin de vérifier l'identité du client ou du bénéficiaire effectif;
- l'obtention d'informations supplémentaires sur la nature envisagée de la relation d'affaires, par exemple en interrogeant les clients sur leurs activités commerciales ou sur les pays ou territoires auxquels ils envisagent de transférer de la monnaie électronique;
- l'obtention d'informations sur le commerçant/bénéficiaire, en particulier lorsque l'émetteur de monnaie électronique a des motifs de soupçonner que ses produits sont utilisés pour acheter des biens illicites ou soumis à une limite d'âge;
- la mise en œuvre de contrôles contre la fraude à l'identité pour s'assurer que le client est bien la personne qu'il affirme être;
- l'exercice d'un contrôle renforcé de la relation client et des transactions individuelles;
- l'établissement de l'origine et/ou de la destination des fonds.

Mesures de vigilance simplifiées à l'égard de la clientèle

126. Dans la mesure où cela est autorisé par le droit national, les établissements peuvent envisager d'appliquer des mesures de vigilance simplifiées à l'égard des produits de monnaie électronique à faible risque qui ne bénéficient pas de l'exemption prévue à l'article 12 de la directive (UE) 2015/849.

127. Dans la mesure où cela est autorisé par le droit national, les mesures de vigilance simplifiées à l'égard de la clientèle que les établissements peuvent appliquer dans les situations à faible risque comprennent notamment:

- le report de la vérification de l'identité du client ou du bénéficiaire effectif à une date ultérieure à l'établissement de la relation ou après le dépassement d'un certain seuil monétaire (faible) (lorsque la première de ces deux éventualité est réalisée). Le seuil monétaire ne devrait pas excéder 250 EUR lorsque le produit n'est pas rechargeable ou peut être utilisé dans d'autres pays ou territoires ou pour des transactions transfrontalières, ou 500 EUR lorsque le droit national le permet (dans ce cas, le produit ne peut être utilisé que dans un cadre national);
- la vérification de l'identité du client sur la base d'un paiement débité d'un compte détenu au nom du client, à titre individuel ou joint, ou sur un compte sur lequel le client exerce un contrôle avéré auprès d'un établissement de crédit ou d'un établissement financier réglementé de l'EEE;
- la vérification de l'identité à partir d'un moins grand nombre de sources;
- la vérification de l'identité à partir de sources moins fiables;
- l'utilisation d'autres méthodes pour vérifier l'identité;
- la présomption de la nature et de l'objet envisagé de la relation d'affaires lorsque ceux-ci sont évidents, par exemple dans le cas de certaines cartes cadeaux qui ne relèvent pas de l'exemption en circuit fermé/réseau fermé (closed loop/closed network exemption);
- la réduction de l'intensité des contrôles tant qu'un certain seuil monétaire n'est pas atteint. Le contrôle continu étant un moyen important d'obtenir plus d'informations sur les facteurs de risque liés aux clients (voir ci-dessus) au cours d'une relation avec un client, le seuil pour les transactions individuelles et pour les transactions qui semblent être liées sur une période de 12 mois devrait être fixé à un niveau jugé par l'établissement comme présentant un faible risque de financement du terrorisme et de blanchiment de capitaux.

Chapitre 4: Orientations sectorielles pour les entreprises de transmission de fonds

128. Les entreprises de transmission de fonds sont des établissements de paiement qui sont habilités en vertu de la directive 2007/64/CE à fournir et à exécuter des services de paiement dans l'ensemble de l'UE. Les entreprises évoluant dans ce secteur sont diverses et vont des entreprises individuelles aux exploitants de chaînes complexes.

129. De nombreuses entreprises de transmission de fonds ont recours à des agents agissant en leur nom et pour leur compte pour fournir des services de paiement. Les agents fournissent souvent des services de paiement comme composante annexe à leur activité principale et peuvent ne pas être eux-mêmes des entités assujetties à la législation applicable en matière de lutte contre le BC/FT; dès lors, leur expertise en matière de lutte contre le BC/FT peut être limitée.

130. La nature du service fourni peut exposer les entreprises de transmission de fonds à un risque de BC/FT. Cela est dû à la simplicité et à la rapidité des transactions, à leur portée mondiale et au fait qu'elles reposent souvent sur des paiements en espèces. En outre, en raison de la nature de ce service de paiement, les entreprises de transmission de fonds réalisent souvent des transactions à titre occasionnel avec leurs clients plutôt que d'établir une relation d'affaires, de telle sorte qu'elles peuvent avoir une compréhension limitée du risque de BC/FT associé au client.

131. Les entreprises de transmission de fonds devraient prendre en considération les mesures et les facteurs de risque suivants, ainsi que ceux énoncés au titre II des présentes orientations.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

132. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- le produit permet des transactions d'un montant élevé ou illimité;
- le produit ou le service est de portée mondiale;
- la transaction est basée sur des paiements en espèces ou est financée au moyen de monnaie électronique anonyme, y compris la monnaie électronique bénéficiant de l'exemption prévue à l'article 12 de la directive (UE) 2015/849;
- les transferts sont effectués par un ou plusieurs payeurs dans différents pays au profit d'un bénéficiaire local.

133. Le facteur suivant peut contribuer à une diminution du risque:

- les fonds utilisés dans le transfert proviennent d'un compte détenu au nom du payeur auprès d'un établissement de crédit ou d'un établissement financier de l'EEE.

Facteurs de risque liés aux clients

134. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- L'activité commerciale du client:

  i. Le client possède ou exploite une entreprise qui traite d'importantes sommes en espèces.

  ii. L'entreprise du client possède une structure de propriété complexe.

- Le comportement du client:

  i. Les besoins du client pourraient être mieux servis ailleurs, par exemple parce que l'entreprise de transmission de fonds n'est pas établie dans le même pays ou territoire que le client ou l'entreprise du client.

  ii. Le client semble agir au nom de quelqu'un d'autre, par exemple d'autres personnes surveillent le client ou sont visibles devant le lieu où la transaction est exécutée, ou le client lit des instructions sur une note.

  iii. Le comportement du client ne paraît pas logique sur le plan économique, par exemple le client accepte un taux de change défavorable ou des frais élevés sans poser de conditions, demande une transaction dans une devise qui n'est pas une monnaie officielle ou qui n'est pas communément utilisée dans le pays ou territoire où est établi le client et/ou le destinataire, ou bien demande ou fournit d'importantes sommes de devises étrangères en petites ou grosses coupures.

  iv. Les transactions du client sont toujours juste en dessous des seuils applicables, y compris le seuil des mesures de vigilance à l'égard de la clientèle pour les transactions réalisées à titre occasionnel visées à l'article 11, point b), de la directive (UE) 2015/849, et le seuil de 1 000 EUR prévu à l'article 5, paragraphe 2, du règlement (UE) 2015/847. 28 Les établissements devraient noter que le seuil visé à l'article 5, paragraphe 2, du règlement (UE) 2015/847 s'applique uniquement aux transactions qui ne sont pas effectuées au moyen d'espèces ou de monnaie électronique anonyme.

  v. Le client fait un usage inhabituel du service, par exemple il s'envoie de l'argent ou transfère les fonds immédiatement après les avoir reçus.

  vi. Le client semble avoir peu de connaissances ou est peu enclin à fournir des informations sur le bénéficiaire.

[28] Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) nº 1781/2006 (Texte présentant de l'intérêt pour l'EEE).

vii. Plusieurs des clients de l'établissement transfèrent des fonds au même bénéficiaire ou semblent avoir les mêmes informations d'identification, par exemple l'adresse ou le numéro de téléphone.

viii. Les transactions d'entrée ne sont pas accompagnées des informations requises sur le payeur ou le bénéficiaire.

ix. Le montant envoyé ou reçu ne correspond pas aux revenus du client (lorsqu'ils sont connus).

135. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Le client est un client de longue date de l'établissement dont le comportement passé n'a pas fait naître de soupçons, et rien n'indique que le risque de BC/FT pourrait être revu à la hausse.
- Le montant transféré est faible; toutefois, les établissements devraient noter que les montants faibles ne suffisent pas en eux-mêmes à écarter le risque de financement du terrorisme.

Facteurs de risque liés aux canaux de distribution

136. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- L'instrument de financement ne fait l'objet d'aucune limitation, par exemple dans le cas de paiements en espèces ou de paiements de produits de monnaie électronique bénéficiant de l'exemption visée à l'article 12 de la directive (UE) 2015/849, de virements bancaires ou de chèques.
- Le canal de distribution utilisé garantit un certain niveau d'anonymat.
- Le service est fourni entièrement en ligne sans garanties adéquates.
- Le service de transmission de fonds est fourni par l'intermédiaire d'agents:

i. qui représentent plusieurs mandants;

ii. dont le chiffre d'affaires présente des caractéristiques inhabituelles par rapport à celui d'autres agents dans des lieux similaires, par exemple des transactions d'un volume anormalement élevé ou faible, des paiements en espèces d'un montant inhabituellement élevé ou un nombre élevé de transactions se situant juste en dessous du seuil déclenchant l'application de mesures de vigilance à l'égard de la clientèle, ou qui exécutent des transactions en- dehors des heures d'ouverture normales;

iii. qui effectuent une part importante de leurs transactions avec des payeurs ou des bénéficiaires issus de pays ou territoires associés à un risque plus élevé de BC/FT;

iv. qui semblent avoir des doutes quant à l'application des politiques de lutte contre le BC/FT à l'échelle du groupe, ou qui ne les appliquent pas de manière cohérente; ou

v. qui ne sont pas issus du secteur financier et exercent une autre activité commerciale en tant qu'activité principale.

- Le service de transmission de fonds est fourni par l'intermédiaire d'un vaste réseau d'agents dans différents pays ou territoires.
- Le service de transmission de fonds est fourni par l'intermédiaire d'une chaîne de paiements excessivement complexe, par exemple avec un grand nombre d'intermédiaires opérant dans différents pays ou territoires ou permettant des systèmes de règlement intraçables (formels et informels).

137. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Les agents sont eux-mêmes réglementés par des établissements financiers.
- Le service ne peut être financé qu'au moyen de transferts à partir d'un compte détenu au nom du client auprès d'un établissement de crédit ou d'un établissement financier de l'EEE ou à partir d'un compte sur lequel le client exerce un contrôle avéré.

Facteurs de risque liés aux pays ou zones géographiques

138. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le payeur ou le bénéficiaire est installé dans un pays ou territoire associé à un risque plus élevé de BC/FT.
- Le bénéficiaire réside dans un pays ou territoire ne disposant pas d'un secteur bancaire formel, ou dont le secteur bancaire formel est moins développé, de telle sorte que les services de transmission de fonds informels, tels que le hawala, peuvent être utilisés au point de paiement.

Mesures

139. Étant donné que l'activité de nombre d'entreprises de transmission de fonds est essentiellement fondée sur les transactions, les établissements devraient déterminer quels systèmes de suivi et quels contrôles ils doivent mettre en place pour détecter les tentatives de BC/FT, y compris lorsque les informations dont ils disposent sur les mesures de vigilance à l'égard du client sont limitées ou manquantes, aucune relation d'affaires n'ayant été établie.

140. Les établissements devraient en tout état de cause mettre en place:

- des systèmes permettant d'identifier les transactions liées;
- des systèmes permettant d'identifier si les transactions de différents clients sont destinées au même bénéficiaire;
- des systèmes permettant, dans la mesure du possible, d'établir l'origine et la destination des fonds;
- des systèmes permettant une traçabilité complète tant des transactions que du nombre d'opérateurs inclus dans la chaîne de paiement; et

- des systèmes permettant de s'assurer que, sur toute la chaîne de paiement, seuls ceux qui sont dûment autorisés à fournir des services de transmission de fonds peuvent intervenir.

141. Lorsque le risque associé à une transaction conclue à titre occasionnel ou à une relation d'affaires est accru, les établissements devraient appliquer des mesures de vigilance renforcées à l'égard de la clientèle conformément au titre II, y compris, le cas échéant, un contrôle renforcé des transactions (par exemple en augmentant la fréquence ou en abaissant les seuils). À l'inverse, lorsque le risque associé à une transaction conclue à titre occasionnel ou à une relation d'affaires est faible, et dans la mesure où cela est autorisé par le droit national, les établissements pourraient appliquer des mesures de vigilance simplifiées à l'égard de la clientèle conformément au titre II.

Recours à des agents

142. Les entreprises de transmission de fonds qui ont recours à des agents pour fournir des services de paiement devraient connaître l'identité de leurs agents[29]. Dans ce contexte, les entreprises de transmission de fonds devraient établir et maintenir des politiques et procédures appropriées, fondées sur l'approche par les risques, pour parer au risque que leurs agents puissent se livrer à des activités de BC/FT ou être utilisés pour de telles activités, en prenant notamment les mesures suivantes:

- Identifier la personne qui possède ou contrôle l'agent lorsque celui-ci est une personne morale, afin de s'assurer que le risque de BC/FT auquel est exposée l'entreprise de transmission de fonds par suite du recours à l'agent n'est pas accru.
- Obtenir la preuve, conformément aux exigences visées à l'article 19, paragraphe 1, point c), de la directive (UE) 2015/2366, de l'aptitude et de l'honorabilité des dirigeants et autres personnes responsables de la gestion de l'agent, y compris en prenant en considération leur honnêteté, leur intégrité et leur réputation. Toute demande de renseignements émanant de l'entreprise de transmission de fonds devrait être adaptée à la nature, à la complexité et à l'échelle du risque de BC/FT inhérent aux services de paiement fournis par l'agent et pourrait être fondée sur les procédures de l'entreprise de transmission de fonds concernant les mesures de vigilance à l'égard de la clientèle.
- Prendre des mesures raisonnables pour s'assurer que les contrôles internes de l'agent en matière de lutte contre le BC/FT sont appropriés et qu'ils demeurent appropriés pendant toute la durée de la relation d'agence, par exemple en contrôlant un échantillon des transactions de l'agent ou en examinant les contrôles de l'agent sur place. Lorsque les contrôles internes mis en place par l'agent pour lutter contre le BC/FT diffèrent de ceux de l'entreprise de transmission de fonds, par exemple parce que l'agent représente plusieurs mandants ou parce que l'agent est lui-même une entité assujettie en vertu de la législation applicable en matière de lutte contre le BC/FT, l'entreprise de transmission de fonds devrait évaluer et gérer le risque que ces

[29] Article 19 de la directive (UE) 2366/2015.

différences puissent affecter le respect de ses propres obligations et de celles de l'agent en matière de lutte contre le BC/FT.

- Dispenser une formation aux agents dans le domaine de la lutte contre le BC/FT, afin qu'ils aient une compréhension adéquate des risques de BC/FT auxquels ils sont exposés et de la qualité des contrôles exigée par l'entreprise de transmission de fonds en ce qui concerne la lutte contre le BC/FT.

Chapitre 5: Orientations sectorielles pour la gestion de patrimoine

143. La gestion de patrimoine consiste à fournir des services bancaires et autres services financiers à des individus fortunés ainsi qu'à leurs proches ou entreprises. Elle est également désignée par le terme «banque privée». Les clients d'établissements proposant des services de gestion de patrimoine peuvent attendre du personnel dédié à la gestion de la relation client qu'il leur fournisse des services personnalisés recouvrant notamment les services bancaires (par exemple, comptes courants, crédits immobiliers et devises étrangères), la gestion et le conseil en investissement, les services fiduciaires, le dépôt en garde («safe custody»), l'assurance, les services de «family office», la planification fiscale et successorale, ainsi que les prestations qui y sont associées, y compris l'assistance juridique.

144. La plupart des caractéristiques typiquement associées à la gestion de patrimoine (par exemple, clients fortunés et influents, transactions et portefeuilles d'un montant très élevé, produits et services complexes, y compris des produits d'investissement personnalisés, exigences de confidentialité et de discrétion...) sont indicatives d'un risque de blanchiment de capitaux plus élevé par rapport à celui typiquement présent dans la banque de détail. Les établissements proposant des services de gestion de patrimoine peuvent être particulièrement vulnérables aux abus de clients qui souhaitent dissimuler l'origine de leurs fonds ou, par exemple, échapper à l'imposition dans leur pays ou territoire d'origine.

145. Les établissements évoluant dans ce secteur devraient prendre en considération les mesures et les facteurs de risque suivants, outre ceux exposés au titre II des présentes orientations. Les orientations sectorielles énoncées au titre III, chapitres 2, 7 et 9, pourraient également être pertinentes dans ce contexte.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

146. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- les clients demandent d'importantes sommes en espèces ou d'autres réserves physiques de valeur, telles que des métaux précieux;
- les transactions d'un montant très élevé;
- les arrangements financiers impliquant des pays ou territoires associés à un risque plus élevé de BC/FT (les établissements devraient accorder une attention particulière aux pays qui ont une culture du secret bancaire ou qui ne respectent pas les normes internationales en matière de transparence fiscale);[30]
- les prêts (y compris les crédits immobiliers) garantis par la valeur de biens situés dans d'autres pays ou territoires, en particulier les pays ou territoires où il est difficile de déterminer si le

[30] Voir également le titre II, point 26.

client peut légitimement mettre en œuvre cette garantie, ou lorsque l'identité des parties garantissant le prêt est difficile à vérifier;

- l'utilisation de structures commerciales complexes, telles que les fiducies/trusts ou les véhicules d'investissement privés, en particulier lorsque l'identité du bénéficiaire effectif en dernier ressort pourrait ne pas être claire;
- les activités commerciales exercées dans plusieurs pays, en particulier lorsqu'elles impliquent plusieurs prestataires de services financiers;
- les arrangements transfrontaliers lorsque les actifs sont déposés ou gérés dans un autre établissement financier appartenant au même groupe financier ou extérieur au groupe, en particulier lorsque l'autre établissement financier est installé dans un pays ou territoire associé à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ou territoires présentant des niveaux d'infractions sous-jacentes plus élevés, un dispositif de lutte contre le BC/FT ou des normes de transparence fiscale faibles.

Facteurs de risque liés aux clients

147. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Les clients disposant de revenus et/ou d'un patrimoine issus de secteurs à risque élevé tels que l'armement, les industries extractives, la construction, les jeux d'argent et de hasard ou les entrepreneurs militaires privés.
- Les clients qui ont fait l'objet d'allégations d'infractions crédibles.
- Les clients qui exigent un niveau de confidentialité ou de discrétion inhabituellement élevé.
- Les clients dont le comportement en matière de dépenses et de transactions rend difficile l'établissement d'un type de comportement «normal» ou attendu.
- Les clients très fortunés et influents, y compris les clients qui jouissent d'une grande notoriété publique, les clients non-résidents et les PPE. Lorsqu'un client ou le bénéficiaire effectif d'un client est une PPE, les établissements doivent toujours appliquer des mesures de vigilance renforcées à l'égard de la clientèle, conformément aux articles 18 à 22 de la directive (UE) 2015/849.
- Le client demande à l'établissement de l'aider à obtenir un produit ou service d'un tiers sans logique économique ou commerciale claire.

Facteurs de risque liés aux pays ou zones géographiques[31]

148. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Les activités commerciales sont exercées dans des pays ayant une culture du secret bancaire ou ne respectant pas les normes internationales en matière de transparence fiscale.

[31] Voir également le titre II.

- Le client vit dans un pays ou territoire associé à un risque plus élevé de BC/FT, ou ses fonds proviennent d'une activité exercée dans un tel pays.

Mesures

149. Le membre du personnel chargé de gérer la relation avec le client (le chargé de clientèle) d'un établissement de gestion de patrimoine devrait jouer un rôle central dans l'évaluation du risque. La relation étroite entre le chargé de clientèle et le client facilitera la collecte d'informations permettant de se forger une opinion plus complète de l'objet et de la nature des activités du client (et notamment de comprendre l'origine du patrimoine du client, les raisons pour lesquelles des arrangements complexes ou inhabituels peuvent néanmoins être authentiques et légitimes, ou encore pourquoi des mesures de sécurité supplémentaires pourraient être appropriées). Cette relation étroite peut cependant également entraîner des conflits d'intérêts si le chargé de clientèle développe des liens trop étroits avec le client, au détriment des efforts mis en œuvre par l'établissement pour gérer le risque de criminalité financière. Par conséquent, il conviendra également d'exercer une surveillance indépendante de l'évaluation des risques. Cette surveillance peut être assurée par le service conformité ou par un membre d'un niveau élevé de la hiérarchie, par exemple.

Mesures de vigilance renforcées à l'égard de la clientèle

150. Les mesures suivantes de vigilance renforcées à l'égard de la clientèle pouvant être appropriées dans des situations à haut risque sont les suivantes:

- Obtenir et vérifier davantage d'informations sur les clients que dans des situations où le risque est standard, et réexaminer et mettre à jour ces informations régulièrement ou dès que des modifications significatives sont apportées au profil d'un client. Les établissements devraient procéder à des réexamens en fonction de l'appréciation des risques et réexaminer les clients présentant un risque plus élevé au moins une fois par an ou plus souvent si le risque l'impose. Ces procédures peuvent inclure la consignation des visites effectuées dans les locaux des clients, que ce soit à leur domicile ou sur leur lieu de travail, y compris les éventuelles modifications apportées au profil du client ou d'autres informations susceptibles d'affecter l'évaluation des risques à la suite de ces visites.
- Établir l'origine du patrimoine et des fonds; lorsque le risque est particulièrement élevé et/ou que l'établissement a des doutes concernant la légitimité de l'origine des fonds, vérifier l'origine du patrimoine et des fonds peut être le seul outil adéquat pour atténuer les risques. L'origine des fonds ou du patrimoine peut être vérifiée en se référant, entre autres:

    i. à l'original ou à une copie certifiée conforme d'une fiche de paie récente;

    ii. à une confirmation écrite du salaire annuel signée par un employeur;

    iii. à l'original ou à une copie certifiée conforme d'un contrat de vente de placements ou d'une entreprise, par exemple;

iv. à une confirmation écrite de la vente signée par un avocat ou un notaire;

v. à l'original ou à une copie certifiée conforme d'un testament ou de l'homologation d'un testament;

vi. à une confirmation écrite d'un héritage signée par un avocat, un notaire, un fiduciaire/trustee ou un exécuteur testamentaire;

vii. à une recherche Internet effectuée dans un registre d'entreprises pour confirmer la vente d'une entreprise.

- Établir la destination des fonds.
- Assurer un niveau de vigilance et de surveillance des relations d'affaires plus élevé que celui qui serait normalement exercé dans le cadre de la fourniture de services financiers conventionnels, tels que la banque de détail ou la gestion d'investissements.
- Procéder à un réexamen interne indépendant et, le cas échéant, obtenir d'un membre d'un niveau élevé de la hiérarchie l'approbation de clients nouveaux et de clients existants en fonction d'une appréciation des risques.
- Contrôler les transactions sur une base continue, y compris, si nécessaire, en réexaminant chaque transaction dès qu'elle a lieu afin de détecter toute activité inhabituelle ou suspecte. Ce contrôle peut comprendre des mesures visant à déterminer si l'un des éléments suivants est incompatible avec le profil de risque commercial:

  i. transferts (d'espèces, d'investissements ou d'autres actifs);

  ii. utilisation de virements bancaires;

  iii. changements significatifs dans l'activité;

  iv. transactions impliquant des pays ou territoires associés à un risque plus élevé de BC/FT.

  Les mesures de contrôle peuvent comprendre l'utilisation de seuils et un processus de réexamen approprié selon lequel les comportements inhabituels sont réexaminés sans délai par le personnel chargé de la relation client ou (à partir de certains seuils) par les fonctions conformité ou les principaux dirigeants.

- Contrôler les rapports publics et autres sources de renseignement pour identifier les informations se rapportant aux clients ou aux personnes connues pour leur être étroitement associées, aux entreprises auxquelles ils sont liés, aux cibles d'acquisition potentielles ou aux bénéficiaires tiers au profit desquels le client effectue des paiements.
- S'assurer que les paiements en espèces ou autres réserves physiques de valeur (par exemple les chèques de voyage [travellers' cheques]) sont traités aux guichets des banques uniquement, et jamais par les chargés de clientèle.

- Veiller à ce que l'établissement se soit assuré que l'utilisation de structures commerciales complexes, telles que les fiducies/trusts ou les véhicules d'investissement privés, par un client est effectuée à des fins légitimes et authentiques, et que l'identité du bénéficiaire effectif en dernier ressort est connue.

Mesures de vigilance simplifiées à l'égard de la clientèle

151. Les mesures de vigilance simplifiées ne sont pas appropriées dans le contexte de la gestion de patrimoine.

Chapitre 6: Orientations sectorielles pour les fournisseurs de crédits commerciaux [«Trade Finance providers»]

152. Les crédits commerciaux (*trade finance*) désignent l'organisation d'un paiement afin de faciliter le mouvement de marchandises (et la fourniture de services) à l'intérieur d'un pays ou à l'international. Lorsque des marchandises sont expédiées à l'étranger, l'importateur peut redouter que les produits ne parviennent pas à destination tandis que l'exportateur peut craindre que le paiement ne soit pas effectué. Les crédits commerciaux font jouer aux banques un rôle d'intermédiaire et permettent de limiter ce double risque.

153. Ces financements peuvent prendre diverses formes, par exemple:

- Les opérations à «compte ouvert» ([*open account transactions]*): l'acheteur effectue un paiement après avoir reçu la marchandise. Il s'agit du mode de financement du commerce le plus courant. La nature des marchandises sous-jacentes à l'opération financière est pourtant fréquemment méconnue des banques chargées d'exécuter leur paiement par transfert de fonds Pour gérer le risque associé à de telles opérations, les banques devraient se référer au titre II des présentes orientations.
- Les lettres de crédit (ou crédits documentaires): une lettre de crédit est un instrument financier émis par une banque qui garantit un paiement vis-à-vis d'un bénéficiaire désigné (typiquement un exportateur) sur présentation de certains documents «conformes» énoncés dans les conditions du crédit documentaire (par exemple la preuve de l'expédition des produits).
- Remise documentaire (ou encaissement documentaire): processus par lequel le paiement, ou une lettre de change acceptée, est encaissé par une banque chargée de l'«encaissement» auprès d'un importateur de produits en vue de son reversement à l'exportateur. La banque chargée de l'encaissement remet les documents commerciaux pertinents (reçus préalablement de l'exportateur, normalement par l'intermédiaire de sa banque) à l'importateur contre paiement.

  Les autres types de crédits commerciaux, tels que le «forfaiting» ou le financement structuré, ou encore le financement de projet ne relèvent pas du champ d'application des présentes lignes directrices sectorielles. Les banques qui proposent ces produits devraient se référer aux lignes directrices générales énoncées au titre II.

155. Les produits de financement du commerce peuvent être détournés à des fins de BC/FT. Par exemple, l'acheteur et le vendeur peuvent s'entendre pour déclarer de fausses informations concernant le prix, le type, la qualité ou la quantité de produits de façon à permettre l'envoi de fonds ou de valeurs entre différents pays.

156. La Chambre de commerce internationale (ICC) a élaboré des normes régissant l'utilisation des lettres de crédit et de la remise documentaire, mais ces normes ne portent pas sur les

questions liées à la criminalité financière[32] et ne sont pas juridiquement contraignantes. Leur utilisation n'implique pas que les banques sont exonérées de leurs obligations légales et réglementaires en matière de lutte contre le BC/FT.

157. Les établissements évoluant dans ce secteur devraient prendre en considération les mesures et les facteurs de risque suivants, outre ceux exposés au titre II des présentes lignes directrices. Les lignes directrices sectorielles énoncées au titre III, chapitre 1, pourraient également être pertinentes dans ce contexte.

Facteurs de risque

158. Les banques intervenant dans les transactions de financement du commerce ont souvent un accès limité aux informations relatives à l'opération commerciale et sur les parties à celle-ci. Les documents commerciaux peuvent être très variés, et les banques peuvent ne pas disposer de l'expertise nécessaire concernant les différents types de documents commerciaux qu'elles reçoivent. Cela peut rendre difficile l'identification et l'évaluation du risque de BC/FT.

159. Les banques devraient, néanmoins, faire preuve de bon sens et exercer un jugement professionnel pour apprécier dans quelle mesure les informations et les documents dont elles disposent pourraient susciter des inquiétudes ou faire naître des soupçons de BC/FT.

160. Dans la mesure du possible, les banques devraient prendre en considération les facteurs de risque suivants:

Facteurs de risque liés aux opérations

161. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le montant de l'opération commerciale est inhabituellement élevé au regard de ce que l'on sait des précédentes activités commerciales d'un client.
- L'opération commerciale est fortement structurée, fragmentée ou complexe, impliquant plusieurs parties, sans justification légitime apparente.
- La copie de documents est utilisée dans des situations où l'utilisation de documents originaux serait normale, sans aucune explication raisonnable.
- Des contradictions significatives existent entre les différents documents, par exemple entre la description des produits figurant dans les principaux documents (c'est-à-dire les factures et les documents de transport) et les produits effectivement expédiés.
- Le type, la quantité et la valeur des biens ne correspondent pas à la connaissance des activités commerciales de l'acheteur connues de la banque.

[32] Les règles et usances uniformes relatives aux crédits documentaires (UCP 600) et les règles uniformes relatives à la remise documentaire (URC 522).

- Les biens échangés présentent un risque de BC plus élevé. Par exemple certaines matières premières dont les prix peuvent fluctuer de manière significative, ce qui peut rendre difficile la détection de prix fictifs.
- Les biens échangés nécessitent une licence d'exportation.
- Les documents commerciaux ne sont pas conformes aux lois et normes applicables.
- Les prix à l'unité semblent inhabituels au regard de ce que la banque connait des produits et de l'opération.
- L'opération présente d'autres caractéristiques inhabituelles. Par exemple les lettres de crédit sont fréquemment modifiées sans logique claire, ou les biens expédiés transitent par un autre pays ou territoire sans raison commerciale apparente.

162. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Des agents d'inspection indépendants ont vérifié la qualité et la quantité des biens.
- Les transactions impliquent des contreparties de longue date qui peuvent justifier d'une longue collaboration, et des mesures de vigilance ont été prises précédemment.

Facteurs de risque liés aux clients

163. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- L'opération commerciale et/ou les parties impliquées ne correspondent pas aux éléments de connaissance de la banque liés aux précédentes activités ou au précédent secteur d'activité du client (par exemple, les produits expédiés ou les volumes d'expédition ne correspondent pas à ce qu'elle connaît de l'activité de l'importateur ou de l'exportateur).
- Il existe des indices selon lesquels il pourrait y avoir une entente entre l'acheteur et le vendeur, par exemple:

  i. l'acheteur et le vendeur sont contrôlés par la même personne; les entreprises parties à l'opération commerciale ont la même adresse, fournissent uniquement l'adresse d'un agent enregistré ou présentent d'autres incohérences en ce qui concerne les adresses;

  ii. l'acheteur est prêt à, ou désireux d'accepter ou de renoncer aux écarts constatés dans les documents.

- Le client ne souhaite pas ou n'est pas en mesure de fournir les pièces justificatives pertinentes à l'appui de l'opération.
- L'acheteur a recours à des agents ou à des tiers.

164. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Le client est un client existant dont l'activité est bien connue de la banque et la transaction est cohérente avec cette activité.

- Le client est coté sur un marché boursier soumis à des obligations de déclaration similaires à celles de l'UE.

Facteurs de risque liés aux pays ou zones géographiques

165. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Un pays associé à l'opération (y compris le pays dont sont originaires les produits, le pays auquel ils sont destinés ou celui par lequel ils ont transité, ou le pays dans lequel l'une ou l'autre partie à la transaction est domiciliée) a mis en place un contrôle des changes. Cela augmente le risque que l'opération ait pour véritable objet l'exportation de devises en violation de la législation locale.
- Un pays lié à l'opération présente un plus grand nombre d'infractions sous-jacentes (par exemple celles liées au trafic de drogues, à la contrebande ou à la contrefaçon) ou des zones de libre-échange.

166. Les facteurs suivants peuvent contribuer à une diminution du risque:

- La transaction est effectuée au sein de l'UE/EEE.
- Les pays associés à la transaction disposent d'un dispositif de lutte contre le BC/FT qui n'est pas moins solide que celui requis en application de la directive (UE) 2015/849, et ils sont associés à un nombre d'infractions sous-jacentes faibles.

Mesures

167. Les banques doivent prendre des mesures de vigilance à l'égard du donneur d'ordre. Dans la pratique, la plupart des banques n'accepteront que des ordres émanant de clients connus. Les autres éléments de connaissance recueillis dans le cadre de la relation d'affaires peuvent aider la banque dans ses efforts de vigilance.

168. Lorsqu'une banque fournit des crédits commerciaux à un client, elle devrait appliquer des mesures, dans le cadre de son processus de vigilance à l'égard de la clientèle, pour comprendre les activités de son client. Le type d'informations que la banque pourrait obtenir comprend notamment les pays avec lesquels son client commerce, les routes commerciales utilisées, les biens échangés, les partenaires commerciaux du client (acheteurs, fournisseurs, etc.), le recours à des agents ou à des tiers, et, si tel est le cas, où ceux-ci sont installés. Ces éléments d'information devraient aider les banques à comprendre l'identité du client et à détecter les opérations inhabituelles ou suspectes.

169. Lorsqu'une banque a une relation de correspondance bancaire s elle doit appliquer des mesures de vigilance à l'égard de l'établissement client. Les banques correspondantes devraient suivre les lignes directrices sur les relations bancaires de correspondant énoncées au titre III, chapitre 1.

Mesures de vigilance renforcées à l'égard de la clientèle

170. Dans les situations à plus haut risque, les banques devraient appliquer des mesures de vigilance renforcées à l'égard de leur clientèle. Dans ce cadre, elles devraient considérer l'opportunité ou non d'effectuer des vérifications de vigilance plus complètes concernant l'opération elle-même et les autres parties à l'opération (y compris les non clients).

171. Les vérifications à effectuer sur les autres parties à la transaction peuvent comprendre:

- La mise en œuvre de mesures pour mieux comprendre la structure de propriété ou l'environnement des autres parties à l'opération, en particulier lorsque celles-ci sont installées dans un pays ou territoire considéré comme présentant une exposition à un risque plus élevé de BC/FT, ou les parties font le commerce de produits fortement exposé à un risque élevé de BC/FT. Ces mesures peuvent comprendre des vérifications au niveau des registres tenus par les entreprises et autres sources de renseignement, ainsi que des recherches dans des sites d'information publics de l'Internet.
- la collecte d'informations supplémentaires sur la situation financière des parties à l'opération.

172. Les vérifications effectuées sur les caractéristiques des opérations peuvent comprendre:

- L'utilisation de bases de données tierces ou de bases de données ouvertes, par exemple le Bureau Maritime International (pour les avertissements, les connaissements, les vérifications d'expéditions et de prix) ou le service de suivi gratuit des conteneurs de compagnies de transport maritime pour vérifier les informations fournies et pour s'assurer que l'objet de l'opération commerciale est légitime;
- Le recours à un expert professionnel pour déterminer si le prix des produits est cohérent sur un plan commercial, en particulier en ce qui concerne les échanges de matières premières pour lesquelles des informations fiables et actualisées peuvent être obtenues;
- la vérification que les poids et volumes des produits expédiés sont compatibles avec le mode de transport utilisé.

173. Étant donné que les lettres de crédit et les encaissements documentaires sont généralement établis sur papier et accompagnés de documents commerciaux (par exemple les factures, connaissements et manifestes), le contrôle automatisé des opérations pourrait ne pas être possible. La banque en charge du financement devrait s'assurer que les documents recueillis sont conformes aux conditions de l'opération commerciale et exiger du personnel qu'il s'appuie sur son expertise et son jugement professionnel pour déterminer si des éléments inhabituels justifient l'application de mesures de vigilance renforcées à l'égard du client ou font naître un soupçon de BC/FT[33].

[33] Les banques vérifient systématiquement les documents pour détecter toute tentative de fraude vis-à-vis d'elle-même ou de leur client. Ces vérifications constituent une composante essentielle du service fourni par une banque spécialisée dans la fourniture de crédits commerciaux. Les banques pourraient s'appuyer sur les contrôles existants pour remplir leurs obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Mesures de vigilance simplifiées à l'égard de la clientèle

174. Les vérifications que les banques effectuent régulièrement pour détecter la fraude et veiller à ce que l'opération respecte les règles fixées par la Chambre de Commerce Internationale conduisent en pratique, à ce qu'elles n'appliquent pas de mesures de vigilance simplifiées à l'égard de leur clientèle, même dans les situations présentant un risque moins élevé.

Chapitre 7: Orientations sectorielles pour les entreprises d'assurance vie

175. Les produits d'assurance vie sont destinés à protéger financièrement le preneur d'assurance contre le risque d'un évènement futur incertain, tel que le décès, la maladie ou l'épuisement de l'épargne constituée en vue de la retraite (risque de longévité). La protection est assurée par un assureur qui met en commun les risques financiers auxquels un grand nombre de preneurs d'assurance différents sont exposés. Les produits d'assurance vie peuvent également être souscrits en tant que produits d'investissement ou pour la retraite.

176. Les produits d'assurance vie sont fournis par le biais de différents canaux de distribution à des clients qui peuvent être des personnes physiques ou morales ou des constructions juridiques. Le bénéficiaire du contrat peut être le preneur d'assurance ou un tiers nommé ou désigné par celui-ci; le bénéficiaire peut également être modifié pendant la durée du contrat et le bénéficiaire initial peut ne jamais percevoir les prestations.

177. La plupart des produits d'assurance vie sont conçus pour le long terme et certains produits ne verseront les prestations qu'après la survenue d'un évènement vérifiable, tel que le décès ou la retraite. Cela signifie que de nombreux produits d'assurance vie ne sont pas assez flexibles pour être le véhicule de prédilection des blanchisseurs de capitaux. Toutefois, comme pour d'autres produits et services financiers, il existe un risque que les fonds utilisés pour souscrire une assurance vie proviennent d'une activité criminelle.

178. Les établissements évoluant dans ce secteur devraient prendre en considération les mesures et les facteurs de risque suivants, outre ceux exposés au titre II des présentes orientations. Les orientations sectorielles énoncées au titre III, chapitres 5 et 9, peuvent également être pertinentes dans ce contexte. En cas de recours à des intermédiaires, les facteurs de risque liés aux canaux de distribution énoncés au titre II, points 32 et 33, sont pertinents.

179. Les présentes orientations peuvent également être utiles aux intermédiaires.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

180. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- La flexibilité des paiements, par exemple le fait que le produit permet:

  i. les paiements en provenance de tiers non identifiés;

  ii. les paiements de primes d'un montant élevé ou illimité, les paiements excédentaires ou les volumes importants de paiements de primes d'un montant plus faible;

  iii. les paiements en espèces.

- La facilité d'accès aux sommes accumulées sur le contrat, par exemple le fait que le produit permet les rachats partiels ou le rachat total anticipé à tout moment, avec des frais limités.

- La négociabilité, par exemple le fait que produit peut être:

  iv. négocié sur un marché secondaire;

  v. utilisé comme garantie d'un prêt.

- L'anonymat, par exemple le fait que le produit favorise ou permet l'anonymat du client.

181. Les facteurs qui peuvent contribuer à une diminution du risque comprennent notamment : Le produit:

- ne verse les prestations qu'en cas de survenue d'un événement prédéfini, par exemple en cas de décès, ou à une date spécifique, par exemple dans le cas de contrats d'assurance vie qui couvrent les crédits à la consommation et les prêts immobiliers et ne versent les prestations qu'au décès de l'assuré;
- n'a pas de valeur de rachat;
- n'a pas d'élément d'investissement;
- n'est pas assorti d'une facilité de paiement par des tiers;
- nécessite que l'investissement total soit réduit à une faible valeur;
- est un contrat d'assurance vie dont la prime est faible;
- ne permet que les paiements de primes réguliers d'un faible montant, et non les paiements excédentaires par exemple;
- n'est accessible que via un employeur, par exemple un régime de retraite ou dispositif similaire versant des prestations de retraite aux employés, pour lequel les cotisations se font par déduction du salaire et dont les règles ne permettent pas aux bénéficiaires de transférer leurs droits;
- ne peut être racheté à court ou moyen terme, comme dans le cas des contrats d'assurance retraite qui ne comportent pas de clause de rachat anticipé;
- ne peut pas être utilisé comme garantie;
- ne permet pas les paiements en espèces;
- est assorti de conditions qui doivent être respectées pour bénéficier des avantages fiscaux.

Facteurs de risque liés aux clients et aux bénéficiaires

182. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- La nature du client, par exemple:

  i. les personnes morales dont la structure rend l'identification du bénéficiaire effectif difficile;

ii. le client ou le bénéficiaire effectif du client est une PPE;

iii. le bénéficiaire du contrat ou le bénéficiaire effectif de ce bénéficiaire est une PPE;

iv. l'âge du client est inhabituel par rapport au type de produit demandé (par exemple le client est très jeune ou très vieux);

v. IV. le contrat ne correspond pas à la situation patrimoniale du client;

vi. la profession ou les activités du client sont considérées comme particulièrement susceptibles d'être liées au blanchiment de capitaux, par exemple parce qu'elles sont connues pour nécessiter beaucoup d'espèces ou être exposées à un risque de corruption élevé;

vii. le contrat est souscrit par un «gardien» (*gatekeeper*), tel qu'une société fiduciaire, agissant au nom du client;

viii. le preneur d'assurance et/ou le bénéficiaire du contrat sont des sociétés dont le capital est détenu par des actionnaires apparents («nominee shareholders») et/ou représenté par des actions au porteur.

- Le comportement du client:

i. En ce qui concerne le contrat, par exemple:

a. le client transfère fréquemment le contrat d'un assureur à un autre;

b. le client effectue des rachats fréquents et inexpliqués, en particulier lorsque le remboursement est effectué sur différents comptes bancaires;

c. le client fait un usage fréquent ou inattendu de la faculté de renonciation (free look provisions) et/ou des périodes de réflexion (cooling-off periods), en particulier lorsque le remboursement est effectué au bénéfice d'un tiers sans lien apparent avec le client;[34]

d. le client encourt des frais élevés en demandant la résiliation anticipée d'un produit;

e. le client transfère le contrat à un tiers sans lien apparent;

f. la demande du client visant à modifier ou à augmenter le montant assuré et/ou le paiement de primes est inhabituelle ou excessive.

ii. En ce qui concerne le bénéficiaire, par exemple:

[34] Une faculté de renonciation est une disposition contractuelle souvent obligatoire en vertu de la législation locale, qui permet au titulaire d'un contrat d'assurance vie ou d'un contrat de rente d'examiner le contrat pendant un certain nombre de jours et de le retourner en vue d'un remboursement complet.

a. l'assureur n'est informé d'un changement de bénéficiaire que lorsque la demande de paiement est effectuée;

b. le client modifie la clause de bénéficiaire et désigne un tiers sans lien apparent;

c. l'assureur, le client, le bénéficiaire effectif, le bénéficiaire ou le bénéficiaire effectif du bénéficiaire sont établis dans des pays ou territoires différents.

iii. En ce qui concerne les paiements, par exemple:

a. le client utilise des méthodes de paiement inhabituelles, telles que des paiements en espèces ou des instruments monétaires structurés, ou d'autres instruments de paiement favorisant l'anonymat;

b. des paiements effectués à partir de différents comptes bancaires sans explication;

c. des paiements provenant de banques qui ne sont pas établies dans le pays de résidence du client;

d. le client effectue des paiements excédentaires fréquents ou d'un montant élevé alors même que cela n'était pas prévu;

e. des paiements reçus de tiers non liés;

f. des versements de rattrapage effectués sur un plan de retraite à l'approche de la date de la retraite.

183. Les facteurs suivants peuvent contribuer à une diminution du risque:

Dans le cas des contrats d'assurance vie détenus par des entreprises, le client est:

- un établissement de crédit ou un établissement financier qui est soumis à des obligations de lutte contre le BC/FT et qui fait l'objet d'une surveillance conforme à la directive (UE) 2015/849 afin de s'assurer du respect de ces obligations;
- une société cotée sur un marché boursier et soumise à des obligations d'information réglementaires (que ce soit par les règles du marché boursier, ou par la loi ou un dispositif contraignant), comportant l'obligation d'assurer une transparence suffisante des bénéficiaires effectifs, ou une filiale détenue majoritairement par cette société;
- une administration ou une entreprise publique d'un pays ou territoire de l'EEE.

Facteurs de risque liés aux canaux de distribution

184. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- les ventes qui n'impliquent pas la présence physique des parties, telles que les ventes en ligne, postales ou par téléphone, et qui ne sont pas assorties de garanties adéquates, telles qu'une signature électronique ou des documents d'identification conformes au règlement (UE) nº 910/2014;

- les longues chaînes d'intermédiaires;
- le recours à un intermédiaire dans des circonstances inhabituelles (par exemple, distance géographique inexpliquée).

185. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Les intermédiaires sont bien connus de l'assureur, qui s'est assuré que l'intermédiaire applique des mesures de vigilance à l'égard de la clientèle proportionnées au risque associé à la relation et conformes à celles requises en application de la directive (UE) 2015/849.
- Le produit n'est à la disposition que des employés de certaines entreprises qui ont conclu un contrat avec l'assureur pour la fourniture de produits d'assurance vie à ses employés, par exemple dans le cadre des avantages sociaux proposés par l'entreprise.

Facteurs de risque liés aux pays ou zones géographiques

186. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- L'assureur, le client, le bénéficiaire effectif, le bénéficiaire ou le bénéficiaire effectif du bénéficiaire sont établis dans, ou associés à, des pays ou territoires associés à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ou territoires ne disposant pas de mécanismes de surveillance efficaces en matière de lutte contre le BC/FT.
- Les primes sont payées par le biais de comptes détenus auprès d'établissements financiers établis dans des pays ou territoires associés à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ou territoires ne disposant pas de mécanismes de surveillance efficaces en matière de lutte contre le BC/FT.
- L'intermédiaire est installé dans, ou associé à, des pays ou territoires associés à un risque plus élevé de BC/FT. Les établissements devraient accorder une attention particulière aux pays ne disposant pas de mécanismes de surveillance efficaces en matière de lutte contre le BC/FT.

187. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Les pays sont identifiés par des sources crédibles, telles que des évaluations mutuelles ou des rapports d'évaluation détaillés, comme étant dotés de systèmes efficaces de lutte contre le BC /FT
- Les pays sont identifiés par des sources crédibles comme présentant des niveaux faibles de corruption ou d'autre activité criminelle.

Mesures

188. L'article 13, paragraphe 5, de la directive (UE) 2015/849 dispose que, dans le cas de l'assurance vie, les établissements doivent appliquer des mesures de vigilance non seulement à l'égard du client et du bénéficiaire effectif, mais aussi à l'égard des bénéficiaires dès que ceux-ci sont identifiés ou désignés. Cela signifie que les établissements doivent:

- obtenir le nom du bénéficiaire lorsqu'une personne physique ou morale ou une construction juridique est identifiée comme le bénéficiaire; ou
- obtenir suffisamment d'informations pour s'assurer que l'identité des bénéficiaires peut être établie au moment du versement des prestations lorsque les bénéficiaires sont une catégorie de personnes ou sont désignés par certaines caractéristiques. Par exemple, lorsque le bénéficiaire est désigné comme «mes futurs petits-enfants», l'assureur pourrait obtenir des informations sur les enfants du preneur d'assurance.

189. Les établissements doivent vérifier l'identité des bénéficiaires au plus tard au moment du versement des prestations.

190. Lorsque l'établissement sait que l'assurance vie a été transférée à un tiers qui recevra la valeur du contrat, il doit identifier le bénéficiaire effectif lors du transfert.

Mesures de vigilance renforcées à l'égard de la clientèle

191. Les mesures suivantes de vigilance renforcée à l'égard de la clientèle peuvent être appropriées dans une situation à haut risque:

- Lorsque le client fait usage de la «faculté de renonciation/de «réflexion», la prime devrait être remboursée sur le compte bancaire du client à partir duquel les fonds ont été payés. Les établissements devraient veiller à vérifier l'identité du client conformément à l'article 13 de la directive (UE) 2015/849 avant d'effectuer un remboursement, en particulier lorsque la prime est élevée ou que les circonstances semblent inhabituelles. Les établissements devraient également déterminer si l'annulation fait naître un soupçon concernant la transaction et s'il convient ou non de transmettre une déclaration de transaction suspecte.
- Des mesures supplémentaires peuvent être prises pour renforcer les connaissances de l'établissement concernant le client, le bénéficiaire effectif, le bénéficiaire ou le bénéficiaire effectif du bénéficiaire, ainsi que les payeurs et bénéficiaires tiers. Exemples de mesures à prendre:

    i. ne pas utiliser la dérogation visée à l'article 14, paragraphe 2, de la directive (UE) 2015/849, qui prévoit une exemption des mesures de vigilance initiales à l'égard de la clientèle;

vérifier l'identité des autres parties concernées, y compris les payeurs et bénéficiaires tiers, avant le début de la relation d'affaires;
obtenir des informations supplémentaires pour établir l'objet envisagé de la relation d'affaires;
obtenir des informations supplémentaires sur le client et mettre à jour plus régulièrement les données d'identification du client et du bénéficiaire effectif;
si le payeur est différent du client, établir la raison de cette différence;
vérifier les identités sur la base de plusieurs sources fiables et indépendantes;
établir l'origine du patrimoine et l'origine des fonds du client, par exemple grâce à des informations relatives à l'emploi et au salaire, aux règlements de succession ou de divorce;

dans la mesure du possible, identifier le bénéficiaire au début de la relation d'affaires, plutôt que d'attendre qu'il soit identifié ou désigné, compte tenu du fait que le bénéficiaire peut changer pendant la durée du contrat;
identifier et vérifier l'identité du bénéficiaire effectif du bénéficiaire;
conformément aux articles 20 et 21 de la directive (UE) 2015/849, prendre des mesures pour déterminer si le client est une PPE et prendre des mesures raisonnables pour déterminer si le bénéficiaire ou le bénéficiaire effectif du bénéficiaire est une PPE lors du transfert, en totalité ou en partie, du contrat, ou, au plus tard, au moment du versement des prestations;
exiger que le premier paiement soit effectué par le biais d'un compte détenu au nom du client auprès d'une banque soumise à des normes de vigilance à l'égard de la clientèle qui ne sont pas moins solides que celles requises en application de la directive (UE) 2015/849.

192. L'article 20 de la directive (UE) 2015/849 dispose que, lorsque le risque associé à une PPE est élevé, les établissements doivent non seulement appliquer des mesures de vigilance à l'égard de la clientèle, conformément à l'article 13 de la directive, mais aussi informer un membre d'un niveau élevé de leur hiérarchie avant le versement des prestations du contrat afin de permettre à la direction d'avoir un regard averti sur le risque de BC/FT associé à la situation et de décider des mesures les plus appropriées pour atténuer ce risque; en outre, les établissements doivent prendre des mesures de vigilance renforcées à l'égard de l'intégralité de la relation d'affaires.

193. Un contrôle plus fréquent et plus approfondi des transactions peut être nécessaire (y compris, au besoin, établir l'origine des fonds).

Mesures de vigilance simplifiées à l'égard de la clientèle

194. Les mesures suivantes peuvent satisfaire à certaines des exigences de vigilance à l'égard de la clientèle dans les situations à faible risque (dans la mesure où cela est autorisé par le droit national):

- Les établissements pourraient présumer que la vérification de l'identité du client est effectuée sur la base d'un paiement débité d'un compte dont l'établissement sait qu'il est détenu au nom du client, à titre individuel ou conjointement, auprès d'un établissement de crédit réglementé de l'EEE.
- Les établissements pourraient présumer que la vérification de l'identité du bénéficiaire du contrat est effectuée sur la base d'un paiement crédité sur un compte détenu au nom du bénéficiaire auprès d'un établissement de crédit réglementé de l'EEE.

Chapitre 8: Orientations sectorielles pour les entreprises d'investissement

195. La gestion d'investissements consiste à gérer les actifs d'un investisseur dans le but d'atteindre des objectifs d'investissement spécifiques. Elle comprend la gestion discrétionnaire (*discretionary management*), dans le cadre de laquelle les gérants prennent des décisions d'investissement au nom de leurs clients, et la gestion conseil (*advisory management*), dans le cadre de laquelle les gestionnaires d'investissements conseillent leurs clients sur les placements à effectuer mais n'exécutent pas de transactions au nom de leurs clients.

196. Les gestionnaires d'investissements ont généralement un nombre limité de clients privés ou institutionnels, dont beaucoup sont fortunés, par exemple des individus à valeur nette élevée, des fiducies/trusts, des entreprises, des organismes publics et autres véhicules d'investissement. Les fonds des clients sont souvent gérés par un dépositaire local, plutôt que par le gestionnaire d'investissements. Le risque de BC/FT associé à la gestion d'investissements est donc lié principalement au risque associé au type de clients servis par les gestionnaires d'investissements.

197. Les établissements évoluant dans ce secteur devraient prendre en considération les mesures et les facteurs de risque suivants, outre ceux exposés au titre II des présentes orientations. Les orientations sectorielles énoncées au titre III, chapitre 5, peuvent également être pertinentes dans ce contexte.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

198. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- le montant inhabituellement élevé des transactions;
- les paiements de tiers sont possibles;
- le produit ou service est utilisé pour des souscriptions qui sont rapidement suivies de possibilités de rachat, avec une intervention limitée du gestionnaire d'investissements.

Facteurs de risque liés aux clients

199. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le comportement du client, par exemple:

    i. les raisons qui sous-tendent l'investissement ne comportent pas de finalité économique évidente;

le client demande le rachat ou le remboursement d'un placement à long terme dans un délai court après l'investissement initial ou avant la date de remboursement, sans justification claire, en particulier lorsque cela entraîne une perte financière ou le paiement de frais de transaction élevés;

le client demande l'achat et la vente répétés d'actions dans un délai court, sans stratégie ni logique économique évidentes;
le client est réticent à fournir les informations dans le cadre des mesures de vigilance à l'égard du client et du bénéficiaire effectif;
des modifications fréquentes sont apportées aux informations dans le cadre des mesures de vigilance à l'égard de la clientèle ou aux informations de paiement;
le client transfère des fonds dont le montant dépasse celui requis pour l'investissement et demande le remboursement du trop-payé;
les circonstances dans lesquelles le client fait usage de la période de réflexion font naître un soupçon;
le client utilise plusieurs comptes sans notification préalable, en particulier lorsque ces comptes sont détenus dans plusieurs pays ou territoires ou dans des pays ou territoires à haut risque;
le client souhaite structurer la relation de façon à avoir recours à plusieurs parties, par exemple des entreprises apparentes (*nominee companies*), intervenant dans différents pays ou territoires, en particulier lorsque ces pays ou territoires sont associés à un risque plus élevé de BC/FT.

- La nature du client, par exemple:

  i. le client est une entreprise ou une fiducie/un trust établi dans un pays ou territoire associé à un risque plus élevé de BC/FT (les établissements devraient accorder une attention particulière aux pays ou territoires qui ne respectent pas de manière effective les normes internationales en matière de transparence fiscale);

  ii. le client est un véhicule d'investissement qui prend peu ou pas de mesures de vigilance à l'égard de ses propres clients;

  iii. le client est un véhicule d'investissement tiers non réglementé;

  iv. la structure de propriété et de contrôle du client est opaque;

  v. le client ou le bénéficiaire effectif est une personne politiquement exposée ou occupe une autre fonction importante qui pourrait lui permettre d'abuser de sa position à des fins d'enrichissement personnel;

  vi. le client est une entreprise apparente non réglementée dont les actionnaires ne sont pas connus.

- Les activités du client, par exemple les fonds du client, proviennent de secteurs d'activité qui sont associés à un risque de criminalité financière élevé.

200. Les facteurs suivants peuvent contribuer à une diminution du risque:

- Le client est un investisseur institutionnel dont le statut a été vérifié par un organisme gouvernemental de l'EEE, par exemple un régime de retraite agréé par l'État.
- Le client est un organe gouvernemental d'un pays ou territoire de l'EEE.
- Le client est un établissement financier établi dans un pays ou territoire de l'EEE.

Facteurs de risque liés aux pays ou zones géographiques

201. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- L'investisseur ou son dépositaire est installé dans un pays ou territoire associé à un risque plus élevé de BC/FT.
- Les fonds proviennent d'un pays ou territoire associé à un risque plus élevé de BC/FT.

Mesures

202. Les gestionnaires d'investissements doivent de manière générale disposer d'une bonne connaissance de leurs clients afin de les aider à identifier les portefeuilles d'investissement qui leur conviennent. Les informations rassemblées seront comparables à celles obtenues par les établissements aux fins de la lutte contre le BC/FT

203. Dans les situations à plus haut risque, les établissements devraient suivre les orientations exposées au titre II concernant les mesures de vigilance renforcées à l'égard de la clientèle. En outre, lorsque le risque associé à une relation d'affaires est élevé, les établissements devraient:

- identifier et, si nécessaire, vérifier l'identité des investisseurs sous-jacents du client de l'établissement lorsque le client est un véhicule d'investissement tiers non réglementé;
- comprendre la raison de tout paiement ou transfert en provenance ou à destination d'un tiers n'ayant pas fait l'objet de vérifications.

204. Dans la mesure où cela est autorisé par le droit national, les gestionnaires d'investissements peuvent appliquer les orientations énoncées au titre II concernant les mesures de vigilance simplifiées à l'égard de la clientèle dans les situations à faible risque.

Chapitre 9: Orientations sectorielles pour les fournisseurs de fonds d'investissement

205. La fourniture de fonds d'investissement peut impliquer plusieurs parties: le gestionnaire de fonds, les conseillers nommés, le dépositaire et les sous-dépositaires, les agents de registre et, dans certains cas, les courtiers de premier ordre. De la même façon, la distribution de ces fonds peut faire intervenir des parties telles que des agents liés, des gestionnaires de fortune spécialisés en gestion conseil et discrétionnaire, des fournisseurs de services de plateforme et des conseillers financiers indépendants.

206. Le type et le nombre de parties impliquées dans le processus de distribution d'un fonds dépendent de la nature du fonds et peuvent avoir une incidence sur la quantité d'informations dont dispose le fonds sur son client et sur ses investisseurs. Le fonds ou, lorsque le fonds n'est pas lui-même une entité assujettie, le gestionnaire du fonds demeurera responsable du respect des obligations de lutte contre le BC/FT, mais certaines obligations du fonds concernant les mesures de vigilance à l'égard de la clientèle peuvent être exécutées par une ou plusieurs de ces autres parties, sous réserve de certaines conditions.

207. Les fonds d'investissement peuvent être utilisés par des personnes ou des entités à des fins de BC/FT:

- Les fonds de détail («retail funds») sont souvent distribués sans la présence physique des parties; il est souvent facile et relativement rapide d'accéder à ces fonds, et les parts détenues dans ces fonds peuvent être transférées entre différentes parties.
- Les fonds d'investissement alternatifs («alternative Investment funds»), tels que les fonds d'investissement spéculatifs («hedge funds»), les fonds d'investissement immobilier et les fonds de placement du secteur privé («private equity»), font généralement intervenir un nombre d'investisseurs moins restreint, qui peuvent être des particuliers ou des investisseurs institutionnels (fonds de pension, fonds de fonds). Les fonds destinés à un nombre limité d'individus très fortunés ou aux «family offices» peuvent présenter un risque d'abus à des fins de BC/FT intrinsèquement plus élevé que les fonds de détail, dans la mesure où les investisseurs sont davantage susceptibles d'être en mesure d'exercer un contrôle sur les actifs du fonds. Si les investisseurs exercent un contrôle sur les actifs, ces fonds sont des structures de détention d'actifs personnels qui sont mentionnées comme un facteur indicatif d'un risque potentiellement plus élevé à l'annexe III de la directive (UE) 2015/849.
- Bien que l'investissement soit souvent à moyen ou long terme, ce qui peut contribuer à en limiter l'attrait pour le blanchiment de capitaux, ces produits peuvent intéresser les personnes procédant au blanchiment de capitaux en raison de leur capacité à générer de la croissance et des revenus.

208. Ce chapitre s'adresse:

a. aux gestionnaires de fonds d'investissement qui exercent des activités au titre de l'article 3, paragraphe 2, point a), de la directive (UE) 2015/849; et

b. aux fonds d'investissement qui commercialisent leurs parts ou leurs actions en application de l'article 3, paragraphe 2, point d), de la directive (UE) 2015/849.

D'autres parties intervenants dans la fourniture ou la distribution de fonds, par exemple les intermédiaires, sont susceptibles d'être assujetties à des obligations de vigilance à l'égard de la clientèle et devraient se référer aux chapitres pertinents des présentes orientations.

209. Pour les fonds et les gestionnaires de fonds, les orientations sectorielles exposées au titre III, chapitres 1, 7 et 8, peuvent également être pertinentes.

Facteurs de risque

Facteurs de risque liés aux produits, aux services et aux transactions

210. Les facteurs suivants peuvent contribuer à une augmentation du risque associé au fonds:

- Le fonds s'adresse à un nombre limité d'individus ou de «family offices», par exemple un fonds privé ou un fonds à investisseur unique.
- L'investisseur peut souscrire au fonds puis rapidement racheter l'investissement sans s'exposer à des frais administratifs importants.
- Les parts ou actions du fonds peuvent être négociées sans en informer le fonds ou le gestionnaire du fonds au moment de l'opération et, par conséquent, les informations concernant l'investisseur sont divisées entre plusieurs acteurs (comme pour les fonds à capital fixe qui font l'objet de transactions sur des marchés secondaires).

211. Les facteurs suivants peuvent contribuer à une augmentation du risque lié à la souscription:

- La souscription implique des comptes ou des tiers dans plusieurs pays ou territoires, en particulier lorsque ces pays ou territoires sont associés à un risque de BC/FT élevé tel que défini aux points 22 à 27 du titre II des orientations.
- La souscription implique des souscripteurs ou bénéficiaires tiers, en particulier lorsque cela n'est pas prévu.

212. Les facteurs suivants peuvent contribuer à une diminution du risque associé au fonds:

- Les paiements par des tiers ne sont pas autorisés.
- Le fonds n'est ouvert qu'aux petits investisseurs, et les investissements sont plafonnés.

Facteurs de risque liés aux clients

213. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Le comportement du client est inhabituel, par exemple:
    i. Les raisons qui sous-tendent l'investissement ne répondent pas à une stratégie ou à une finalité économique évidente, ou le client effectue des investissements qui ne

correspondent pas à sa situation financière globale, lorsque ces éléments sont connus du fonds ou du gestionnaire du fonds.

Le client demande le rachat ou le remboursement d'un placement dans un délai court après l'investissement initial ou avant la date de versement, sans justification claire,
en particulier lorsque cela entraîne une perte financière ou le paiement de frais de transaction élevés.

Le client demande l'achat et la vente répétés d'actions dans un délai court, sans stratégie ni logique économique évidentes.

Le client transfère des fonds dont le montant dépasse celui requis pour l'investissement et demande le remboursement du trop-payé.

Le client utilise plusieurs comptes sans notification préalable, notamment lorsque ces comptes sont détenus dans plusieurs pays ou territoires ou dans des pays ou territoires associés à un risque plus élevé de BC/FT.

Le client souhaite structurer la relation de façon à avoir recours à plusieurs parties, par exemple des entreprises apparentes («nominee companies») non réglementées, dans différents pays ou territoires, en particulier lorsque ces pays ou territoires sont associés à un risque plus élevé de BC/FT.

Le client modifie subitement le lieu de règlement sans raison, par exemple en modifiant le pays de résidence du client.

Le client et le bénéficiaire effectif sont situés dans des pays ou territoires différents et au moins un de ces pays ou territoires est associé à un risque plus élevé de BC/FT, tel que défini dans la partie générale des orientations.

Les fonds du bénéficiaire effectif ont été générés dans un pays ou territoire associé à un risque plus élevé de BC/FT, en particulier lorsque le pays ou territoire est associé à des niveaux d'infractions sous-jacentes au BC/FT plus élevés.

214. Les facteurs suivants peuvent contribuer à une diminution du risque:

- le client est un investisseur institutionnel dont le statut a été vérifié par un organisme gouvernemental de l'EEE, par exemple un régime de retraite agréé par l'État;
- le client est un établissement situé dans un pays de l'EEE ou dans un pays tiers dont les exigences en matière de lutte contre le BC/FT ne sont pas moins solides que celles requises par la directive (UE) 2015/849.

Facteurs de risque liés aux canaux de distribution

215. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- des canaux de distribution peu clairs ou complexes qui limitent la capacité du fonds à surveiller ses relations d'affaires et à contrôler les transactions. Par exemple le fonds a recours à un grand nombre de sous-distributeurs en vue de la distribution dans des pays tiers;
- le distributeur est implanté dans un pays ou territoire associé à un risque plus élevé de BC/FT, tel que défini dans la partie générale des présentes orientations.

216. Les facteurs suivants peuvent indiquer que le risque est moins élevé:

- Le fonds n'admet qu'un certain type d'investisseur à faible risque, tel que les établissements réglementés investissant en tant que principal (par exemple les entreprises d'assurance vie) ou les régimes de retraite d'entreprise.
- Le fonds ne peut être souscrit et remboursé que par l'intermédiaire d'un établissement, par exemple un intermédiaire financier, dans un pays de l'EEE ou dans un pays tiers dont les exigences en matière de lutte contre le BC/FT ne sont pas moins solides que celles requises par la directive (UE) 2015/849.

Facteurs de risque liés aux pays ou zones géographiques

217. Les facteurs suivants peuvent contribuer à une augmentation du risque:

- Les fonds des investisseurs ont été générés dans des pays ou territoires associés à un risque plus élevé de BC/FT, en particulier dans des pays associés à des niveaux d'infractions sous-jacentes au blanchiment de capitaux plus élevés.
- Le fonds ou le gestionnaire du fonds investit dans des secteurs exposés à un risque de corruption plus élevé (par exemple les industries extractives ou l'industrie de l'armement) dans des pays ou territoires identifiés par des sources crédibles comme présentant des niveaux significatifs de corruption ou d'autres infractions sous-jacentes au BC/FT, en particulier lorsque le fonds est un fonds à investisseur unique ou qu'il dispose d'un nombre limité d'investisseurs.

Mesures

218. Les mesures que les fonds ou les gestionnaires de fonds devraient prendre pour remplir leurs obligations de vigilance à l'égard de la clientèle dépendront des modalités de souscription du fonds par le client ou l'investisseur (lorsque l'investisseur n'est pas le client). Le fonds ou le gestionnaire du fonds devrait également prendre des mesures fondées sur son appréciation des risques pour identifier et vérifier l'identité des personnes physiques éventuelles, qui possèdent ou contrôlent le client en dernier ressort (ou au nom desquelles la transaction est exécutée), par exemple en demandant à l'investisseur potentiel de déclarer, lorsqu'il demande à souscrire au fonds pour la première fois, s'il investit pour son propre compte ou s'il agit en tant qu'intermédiaire investissant au nom d'un tiers.

219. Le client est:

a. une personne physique ou morale qui souscrit directement des parts ou des actions d'un fonds pour son propre compte, et non pour le compte d'autres investisseurs sous-jacents; ou

b. un établissement qui, dans le cadre de son activité économique, souscrit directement des parts ou des actions en son nom, et qui exerce un contrôle sur l'investissement au profit d'un ou de plusieurs tiers en dernier ressort qui ne contrôlent pas l'investissement ou les décisions d'investissement; ou

c. un établissement, par exemple un intermédiaire financier, qui agit en son nom et est le propriétaire officiel des actions ou des parts, mais qui agit pour le compte et suivant les instructions spécifiques d'un ou de plusieurs tiers (par exemple, parce que l'intermédiaire financier est un mandataire («nominee»), un courtier, l'exploitant d'un compte commun («pooled account») multi-clients /d'un compte de type omnibus, ou l'exploitant d'un arrangement similaire de type passif); ou

d. le client d'un établissement, par exemple le client d'un intermédiaire financier, lorsque l'établissement n'est pas le propriétaire officiel des actions ou des parts (par exemple, parce que le fonds d'investissement a recours à un intermédiaire financier pour distribuer les actions ou les parts d'un fonds, et que l'investisseur souscrit des parts ou des actions par l'intermédiaire de l'établissement et l'établissement ne devient pas le propriétaire légal des parts ou des actions).

Mesures de vigilance simplifiées et renforcées à l'égard de la clientèle à prendre dans les situations visées aux points 219a et 219b

220. Dans les situations visées aux points 218a et 218b, les mesures de vigilance renforcées à l'égard de la clientèle qu'un fonds ou un gestionnaire de fonds devrait appliquer dans les situations à haut risque comprennent:

- obtenir des informations supplémentaires sur le client, telles que la réputation et le parcours du client, avant l'établissement de la relation d'affaires;
- prendre des mesures supplémentaires pour vérifier de manière plus approfondie les documents, les données et les informations obtenues;
- obtenir des informations sur l'origine des fonds et/ou l'origine du patrimoine du client et du bénéficiaire effectif du client;
- exiger que le remboursement soit effectué par le biais du compte initial utilisé pour l'investissement ou d'un compte détenu au nom du client à titre individuel ou joint;
- augmenter la fréquence et l'intensité du contrôle des transactions;
- exiger que le premier paiement soit effectué par le biais d'un compte de paiement détenu au nom du client, à titre individuel ou joint, auprès d'un établissement de crédit ou d'un établissement financier réglementé de l'EEE ou auprès d'un établissement de crédit ou d'un établissement financier réglementé d'un pays tiers dont les exigences en matière de lutte contre le BC/FT ne sont pas moins solides que celles requises en application de la directive (UE) 2015/849;
- obtenir l'autorisation d'un membre d'un niveau élevé de la hiérarchie au moment de la transaction lorsqu'un client utilise un produit ou un service pour la première fois;
- exercer un contrôle renforcé de la relation client et des transactions individuelles.

221. Dans les situations à risque moins élevé, dans la mesure où cela est autorisé par le droit national et à condition que les fonds soient transférés de manière vérifiable vers ou depuis un

compte de paiement détenu au nom du client, à titre individuel ou joint, auprès d'un établissement de crédit ou d'un établissement financier réglementé de l'EEE, le fonds ou le gestionnaire du fonds pourrait appliquer des mesures de vigilance simplifiées à l'égard de la clientèle, par exemple utiliser l'origine des fonds pour remplir certaines des obligations de vigilance à l'égard de la clientèle.

Mesures de vigilance simplifiées et renforcées à l'égard de la clientèle à prendre dans les situations visées au point 219c

222. Dans les situations visées au point 219c, lorsque l'intermédiaire financier est le client du fonds ou du gestionnaire du fonds, le fonds ou le gestionnaire du fonds devrait appliquer des mesures de vigilance fondées sur l'appréciation des risques à l'égard de l'intermédiaire financier. Le fonds ou le gestionnaire du fonds devrait également prendre des mesures fondées sur son appréciation des risques pour identifier et vérifier l'identité des investisseurs sous-jacents de l'intermédiaire financier, dans la mesure où ces investisseurs sont les bénéficiaires effectifs des fonds investis via l'intermédiaire. Dans la mesure où cela est autorisé par droit national, dans les situations à faible risque, les fonds ou les gestionnaires de fonds peuvent appliquer des mesures de vigilance simplifiées à l'égard de la clientèle similaires à celles visées au point 112 des présentes orientations, sous réserve des conditions suivantes:

- L'intermédiaire financier est assujetti à des obligations de lutte contre le BC/FT dans un pays ou territoire de l'EEE ou dans un pays tiers dont les exigences en matière de lutte contre le BC/FT ne sont pas moins solides que celles requises par la directive (UE) 2015/849.
- L'intermédiaire financier fait l'objet d'une surveillance effective en ce qui concerne le respect de ces exigences.
- Le fonds ou le gestionnaire du fonds a pris des mesures fondées sur son appréciation des risques afin de s'assurer que le risque de BC/FT associé à la relation d'affaires est faible, en fonction, notamment, de l'évaluation par le fonds ou le gestionnaire du fonds des activités de l'intermédiaire financier, des types de clients servis par l'entreprise de l'intermédiaire ainsi que des pays ou territoires auxquels l'activité de l'intermédiaire est exposée.
- Le fonds ou le gestionnaire du fonds a pris des mesures fondées sur son appréciation des risques afin de s'assurer que l'intermédiaire applique des mesures de vigilance solides et fondées sur une appréciation des risques à l'égard de sa propre clientèle et des bénéficiaire effectifs de ses clients. Dans ce contexte, le fonds ou le gestionnaire du fonds devrait prendre des mesures fondées sur une appréciation des risques pour évaluer l'adéquation des politiques et procédures de l'intermédiaire en matière de vigilance à l'égard de la clientèle, par exemple en faisant référence aux informations accessibles au public concernant le respect par l'intermédiaire de ses obligations de vigilance ou en assurant la liaison directe avec l'intermédiaire.
- Le fonds ou le gestionnaire du fonds a pris des mesures fondées sur une appréciation des risques pour s'assurer que l'intermédiaire fournira immédiatement sur demande des informations et des documents sur les mesures de vigilance prises à l'égard des investisseurs

sous-jacents, par exemple en incorporant des dispositions pertinentes dans un contrat avec l'intermédiaire ou en analysant par sondage la capacité de l'intermédiaire à fournir des informations sur demande concernant les mesures de vigilance à l'égard de la clientèle.

223. Lorsque le risque est accru, en particulier lorsque le fonds s'adresse à un nombre limité d'investisseurs, des mesures de vigilance renforcées à l'égard de la clientèle doivent être prises qui peuvent comprendre celles exposées au point 220 ci-dessus.

Mesures de vigilance simplifiées et renforcées à l'égard de la clientèle à prendre dans les situations visées au point 219d

224. Dans les situations visées au point 219d, le fonds ou le gestionnaire du fonds devrait appliquer des mesures de vigilance, en fonction d'une appréciation des risques, à l'égard de l'investisseur en dernier ressort en tant que client du fonds ou du gestionnaire du fonds. Pour remplir ses obligations de vigilance à l'égard de la clientèle, le fonds ou le gestionnaire du fonds peut avoir recours à l'intermédiaire conformément à et sous réserve des conditions prévues au chapitre II, section 4, de la directive (UE) 2015/849.

225. Dans où cela est autorisé par le droit national, dans les situations à faible risque, les fonds ou les gestionnaires de fonds peuvent appliquer des mesures de vigilance simplifiées à l'égard de la clientèle. Pour autant que les conditions énumérées au point 222 soient remplies, les mesures de vigilance simplifiées à l'égard de la clientèle peuvent consister en l'obtention par le fonds ou le gestionnaire du fonds de données d'identification du registre des actionnaires du fonds, ainsi que des informations visées à l'article 27, paragraphe 1, de la directive (UE) 2015/849. Le fonds ou le gestionnaire du fonds doit obtenir ces informations de l'intermédiaire dans un délai raisonnable. Le fonds ou le gestionnaire du fonds devrait arrêter ce délai en fonction de l'approche fondée sur les risques.

226. Lorsque le risque est plus élevé, en particulier lorsque le fonds s'adresse à un nombre limité d'investisseurs, des mesures de vigilance renforcées à l'égard de la clientèle doivent être prises qui peuvent comprendre celles exposées au point 220 ci-dessus.

Titre IV – Mise en œuvre

Mise en œuvre

227. Les autorités compétentes et les établissements devraient mettre en œuvre les présentes orientations avant le 26 juin 2018.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2017 37

26/06/2017

Final Guidelines

Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions

The Risk Factors Guidelines

Contents

1. Executive summary

On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive (EU) 2015/849) entered into force. This Directive aims, inter alia, to bring European Union legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the Financial Action Task Force (FATF), an international anti-money laundering standard setter, adopted in 2012.

In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the centre of the European Union's anti-money laundering (AML) and countering financing of terrorism (CFT) regime. It recognises that the risk of money laundering and terrorist financing (ML/TF) can vary and that Member States, competent authorities, and credit and financial institutions within its scope ('firms') have to take steps to identify and assess that risk with a view to deciding how best to manage it.

Articles 17 and 18(4) of Directive (EU) 2015/849 require the European Supervisory Authorities (ESAs) to issue guidelines to support firms with this task and to assist competent authorities when assessing the adequacy of firms' application of simplified and enhanced customer due diligence measures. The aim is to promote the development of a common understanding, by firms and competent authorities across the EU, of what the risk-based approach to AML/CFT entails and how it should be applied.

These guidelines set out factors firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. They also set out how firms can adjust the extent of their customer due diligence (CDD) measures in a way that is commensurate to the ML/TF risk they have identified. The factors and measures described in these guidelines are not exhaustive and firms should consider other factors and measures as appropriate.

These guidelines are divided into two parts:

- Title II is general and applies to all firms. It is designed to equip firms with the tools they need to make informed, risk-based decisions when identifying, assessing and managing the ML/TF risk associated with individual business relationships or occasional transactions.

- Title III is sector-specific and complements the general guidance in Title II. It sets out risk factors that are of particular importance in certain sectors and provides guidance on the risk-sensitive application of CDD measures by firms in those sectors.

These guidelines will help firms identify, assess and manage the ML/TF risk associated with individual business relationships and occasional transactions in a risk-based, proportionate and effective way. They also clarify how competent authorities in the EU expect firms to discharge their obligations in this field.

Neither these guidelines nor the Directive's risk-based approach require firms to refuse to enter into, or terminate, business relationships with entire categories of customers that are associated with higher ML/TF risk.

The ESAs publicly consulted on a version of these guidelines between 22 October 2015 and 22 January 2016. Respondents welcomed the draft guidelines and considered that they would support the development of an effective risk-based approach to AML/CFT across the EU. Some respondents raised concerns about the ability of national competent authorities to apply these guidelines in a consistent manner, stressed the need for the guidelines to be consistent with international AML/CFT standards and asked for clarification regarding the interaction of these guidelines with other provisions in Union law. These concerns have been addressed in these guidelines as appropriate.

These guidelines will apply by 26 June 2018.

Next steps

The ESAs will keep these guidelines under review and update them as appropriate. The first update is likely to occur once amendments to Directive (EU) 2015/849 have been agreed. The ESAs will consult on any changes made to the substance of these guidelines.

2. Background and rationale

On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive (EU) 2015/849) entered into force. This Directive aims, inter alia, to bring European Union legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the FATF, an international AML/CFT standard setter, adopted in 2012.

In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the centre of European Union's AML/CFT regime. It recognises that the risk of ML/TF can vary and that Member States, competent authorities and obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it.

For obliged entities, CDD is central to this process, for both risk assessment and risk management purposes. CDD means:

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identifying the customer's beneficial owner and taking reasonable measures to verify their identity so that the obliged entity is satisfied that it knows who the beneficial owner is;
- assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- conducting ongoing monitoring of the business relationship. This includes transaction monitoring and keeping the underlying information up to date.[1]

Directive (EU) 2015/849 provides that obliged entities can determine the extent of these measures on a risk-sensitive basis. It also provides that where the risk associated with the business relationship or occasional transaction is low, Member States may allow obliged entities to apply simplified customer due diligence (SDD) measures instead. Conversely, where the risk associated with the business relationship or occasional transaction is increased, obliged entities must apply enhanced customer due diligence (EDD) measures. However, the Directive does not set out in detail how obliged entities should assess the risk associated with a business relationship or transaction, nor does it set out exactly what SDD and EDD measures entail.

The Directive therefore requires the ESAs to issue guidelines to competent authorities and firms on 'the risk factors to be taken into consideration and/or the measures to be taken' in situations

[1] Article 13(1) of Directive (EU) 2015/849.

where SDD or EDD measures are appropriate. These guidelines have to be adopted within two years of the Directive entering into force, that is, no later than 26 June 2017.

These guidelines will support the development of a common understanding, by firms and competent authorities across the EU, of what the risk-based approach to AML/CFT entails and how it should be applied. They will help firms identify, assess and manage the ML/TF risk associated with individual business relationships and occasional transactions in a risk-based, proportionate and effective way.

Neither these guidelines nor the Directive's risk-based approach require the wholesale exiting of entire categories of customers irrespective of the ML/TF risk associated with individual business relationships or occasional transactions.

Countering the financing of terrorism

Many of the CFT measures firms have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison with the authorities. The guidance provided in these guidelines therefore applies to CFT as it does to AML, even where this is not explicitly mentioned.

There are, however, key differences between preventing money laundering and countering the finance of terrorism: the money launderer seeks to disguise the origins of illicit funds, while, in contrast, a person funding terrorism may also use legitimately held funds to pursue illegal aims. Firms should bear this in mind when assessing the risks posed to the firm by those funding terrorism.

A firm's steps to counter the financing of terrorism will include its compliance with financial sanctions directed at people or organisations sanctioned for reasons related to terrorism. The European financial sanctions regime is not covered by Directive (EU) 2015/849 and compliance with this regime is not subject to a risk-based approach. It therefore falls outside the scope of these guidelines.

3. Joint guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (the Risk Factors Guidelines)

Status of these joint guidelines

This document contains joint guidelines issued pursuant to Articles 16 and 56(1) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC; Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority); and Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority) (the European Supervisory Authorities (ESAs) Regulations). In accordance with Article 16(3) of the ESAs Regulations, competent authorities and financial institutions must make every effort to comply with the guidelines.

Joint guidelines set out the ESAs' view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities to whom the joint guidelines apply should comply by incorporating them into their supervisory practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where the joint guidelines are directed primarily at institutions.

Reporting requirements

In accordance with Article 16(3) of the ESAs Regulations, competent authorities must notify the relevant ESA of whether they comply or intend to comply with these joint guidelines, or otherwise of reasons for non-compliance, [*two months after the publication of all translations on the ESAs' websites*]. In the absence of any notification by this deadline, competent authorities will be considered by the relevant ESA to be non-compliant. Notifications should be sent to [compliance@eba.europa.eu, compliance@eiopa.europa.eu and compliance@esma.europa.eu] with the reference 'JC/GL/2017/34'. A template for notifications is available on the ESAs' websites. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities.

Notifications will be published on the ESAs' websites, in line with Article 16(3).

Title I – Subject matter, scope and definitions

Subject matter

1. These guidelines set out factors firms should consider when assessing the money laundering and terrorist financing (ML/TF) risk associated with a business relationship or occasional transaction. They also set out how firms should adjust the extent of their customer due diligence (CDD) measures in a way that is commensurate to the ML/TF risk they have identified.

2. These guidelines focus on risk assessments of individual business relationships and occasional transactions, but firms may use these guidelines *mutatis mutandis* when assessing ML/TF risk across their business in line with Article 8 of Directive (EU) 2015/849.

3. The factors and measures described in these guidelines are not exhaustive and firms should consider other factors and measures as appropriate.

Scope

4. These guidelines are addressed to credit and financial institutions as defined in Article 3(1) and 3(2) of Directive (EU) 2015/849 and competent authorities responsible for supervising these firms' compliance with their anti-money laundering and counter-terrorist financing (AML/CFT) obligations.

5. Competent authorities should use these guidelines when assessing the adequacy of firms' risk assessments and AML/CFT policies and procedures.

6. Competent authorities should also consider the extent to which these guidelines can inform the assessment of the ML/TF risk associated with their sector, which forms part of the risk-based approach to supervision. The ESAs have issued guidelines on risk-based supervision in accordance with Article 48(10) of Directive (EU) 2015/849.

7. Compliance with the European financial sanctions regime is outside the scope of these guidelines.

Definitions

8. For the purpose of these guidelines, the following definitions shall apply:

   - 'Competent authorities' means the authorities competent for ensuring firms' compliance with the requirements of Directive (EU) 2015/849 as transposed by national legislation.[2]

[2] Article 4(2)(ii), Regulation (EU) No 1093/2010; Article 4(2)(ii), Regulation (EU) No 1094/2010; Article 4(3)(ii), Regulation (EU) No 1093/2010.

- 'Firms' means credit and financial institutions as defined in Article 3(1) and (2) of Directive (EU) 2015/849.

- 'jurisdictions associated with higher ML/TF risk' means countries that, based on an assessment of the risk factors set out in Title II of these guidelines, present a higher ML/TF risk. This term includes, but is not limited to, 'high-risk third countries' identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union's financial system (Article 9 of Directive (EU) 2015/849).

- 'Occasional transaction' means a transaction that is not carried out as part of a business relationship as defined in Article 3(13) of Directive (EU) 2015/849.

- 'Pooled account' means a bank account opened by a customer, for example a legal practitioner or notary, for holding their clients' money. The clients' money will be commingled, but clients will not be able directly to instruct the bank to carry out transactions.

- 'Risk' means the impact and likelihood of ML/TF taking place. Risk refers to inherent risk, that is, the level of risk that exists before mitigation. It does not refer to residual risk, that is, the level of risk that remains after mitigation.

- 'Risk factors' means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction.

- 'Risk-based approach' means an approach whereby competent authorities and firms identify, assess and understand the ML/TF risks to which firms are exposed and take AML/CFT measures that are proportionate to those risks.

- 'Source of funds' means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, for example the customer's salary, as well as the means through which the customer's funds were transferred.

- 'Source of wealth' means the origin of the customer's total wealth, for example inheritance or savings.

Title II – Assessing and managing risk: general

9. These guidelines come in two parts. Title II is general and applies to all firms. Title III is sector-specific. Title III is incomplete on its own and should be read in conjunction with Title II.

10. Firms' approach to assessing and managing the ML/TF risk associated with business relationships and occasional transactions should include the following:

- Business-wide risk assessments.

  Business-wide risk assessments should help firms understand where they are exposed to ML/TF risk and which areas of their business they should prioritise in the fight against ML/TF. To that end, and in line with Article 8 of Directive (EU) 2015/849, firms should identify and assess the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers. The steps firms take to identify and assess ML/TF risk across their business must be proportionate to the nature and size of each firm. Firms that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated risk assessment.

- Customer due diligence.

  Firms should use the findings from their business-wide risk assessment to inform their decision on the appropriate level and type of CDD that they will apply to individual business relationships and occasional transactions.

  Before entering into a business relationship or carrying out an occasional transaction, firms should apply initial CDD in line with Article 13(1)(a), (b) and (c) and Article 14(4) of Directive (EU) 2015/849. Initial CDD should include at least risk-sensitive measures to:

  i. identify the customer and, where applicable, the customer's beneficial owner or legal representatives;

  ii. verify the customer's identity on the basis of reliable and independent sources and, where applicable, verify the beneficial owner's identity in such a way that the firm is satisfied that it knows who the beneficial owner is; and

  iii. establish the purpose and intended nature of the business relationship.

  Firms should adjust the extent of initial CDD measures on a risk-sensitive basis. Where the risk associated with a business relationship is low, and to the extent permitted by national legislation, firms may be able to apply simplified customer due diligence measures (SDD). Where the risk associated with a business relationship is increased, firms must apply enhanced customer due diligence measures (EDD).

- Obtaining a holistic view.

Firms should gather sufficient information to be satisfied that they have identified all relevant risk factors, including, where necessary, by applying additional CDD measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship or occasional transaction. Firms should note that the risk factors listed in these guidelines are not exhaustive, and that there is no expectation that firms will consider all risk factors in all cases.

- Monitoring and review.

Firms must keep their risk assessment up to date and under review.[3] Firms must monitor transactions to ensure that they are in line with the customer's risk profile and business and, where necessary, examine the source of funds, to detect possible ML/TF. They must also keep the documents, data or information they hold up to date, with a view to understanding whether the risk associated with the business relationship has changed.[4]

Risk assessments: methodology and risk factors

11. A risk assessment should consist of two distinct but related steps:

a) the identification of ML/TF risk; and

b) the assessment of ML/TF risk.

Identifying ML/TF risk

12. Firms should find out which ML/TF risks they are, or would be, exposed to as a result of entering into a business relationship or carrying out an occasional transaction.

13. When identifying ML/TF risks associated with a business relationship or occasional transaction, firms should consider relevant risk factors including who their customer is, the countries or geographical areas they operate in, the particular products, services and transactions the customer requires and the channels the firm uses to deliver these products, services and transactions.

Sources of information

14. Where possible, information about these ML/TF risk factors should come from a variety of sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. Firms should determine the type and numbers of sources on a risk-sensitive basis.

[3] Article 8(2) of Directive (EU) 2015/849.

[4] Article 13(1)(d) of Directive (EU) 2015/849.

15. Firms should always consider the following sources of information:

- the European Commission's supranational risk assessment;
- information from government, such as the government's national risk assessments, policy statements and alerts, and explanatory memorandums to relevant legislation;
- information from regulators, such as guidance and the reasoning set out in regulatory fines;
- information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and
- information obtained as part of the initial CDD process.

16. Other sources of information firms may consider in this context may include, among others:

- the firm's own knowledge and professional expertise;
- information from industry bodies, such as typologies and emerging risks;
- information from civil society, such as corruption indices and country reports;
- information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists;
- information from credible and reliable open sources, such as reports in reputable newspapers;
- information from credible and reliable commercial organisations, such as risk and intelligence reports; and
- information from statistical organisations and academia.

Risk factors

17. Firms should note that the following risk factors are not exhaustive, nor is there an expectation that firms will consider all risk factors in all cases. Firms should take a holistic view of the risk associated with the situation and note that, unless Directive (EU) 2015/849 or national legislation states otherwise, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

Customer risk factors

18. When identifying the risk associated with their customers, including their customers' beneficial owners,[5] firms should consider the risk related to:

    a) the customer's and the customer's beneficial owner's business or professional activity;

    b) the customer's and the customer's beneficial owner's reputation; and

    c) the customer's and the customer's beneficial owner's nature and behaviour.

19. Risk factors that may be relevant when considering the risk associated with a customer's or a customer's beneficial owner's business or professional activity include:

- Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement?

- Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?

- Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

- Where the customer is a legal person or a legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?

- Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? Where a customer or their beneficial owner is a PEP, firms must always apply EDD measures in line with Article 20 of Directive (EU) 2015/849.

- Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?

- Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly

[5] For guidance on risk factors associated with beneficiaries of life insurance policies, please refer to Title III, Chapter 7.

available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

- Is the customer a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?

- Is the customer a public administration or enterprise from a jurisdiction with low levels of corruption?

- Is the customer's or the beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?

20. The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owners' reputation:

- Are there adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. Firms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

- Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

- Does the firm know if the customer or beneficial owner has been the subject of a suspicious transactions report in the past?

- Does the firm have any in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

21. The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owner's nature and behaviour; firms should note that not all of these risk factors will be apparent at the outset; they may emerge only once a business relationship has been established:

- Does the customer have legitimate reasons for being unable to provide robust

evidence of their identity, perhaps because they are an asylum seeker?[6]

- Does the firm have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

- Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?

- Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

- Does the customer issue bearer shares or does it have nominee shareholders?

- Is the customer a legal person or arrangement that could be used as an asset-holding vehicle?

- Is there a sound reason for changes in the customer's ownership and control structure?

- Does the customer request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade specific thresholds such as those set out in Article 11(b) of Directive (EU) 2015/849 and national law where applicable?

- Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to want to disguise the true nature of their business?

- Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments? Is the explanation plausible?

- Does the customer use the products and services they have taken out as expected when the business relationship was first established?

- Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the customer requesting the type of financial service sought? Firms should note that Article 16 of Directive 2014/92/EU creates a right for customers who are legally resident in the Union to obtain a basic payment account, but this right applies only to the extent that

[6] The EBA has issued an 'Opinion on the application of Customer Due Diligence Measures to customers who are asylum seekers from higher risk third countries or territories', see https://eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf.

credit institutions can comply with their AML/CFT obligations.[7]

- Is the customer a non-profit organisation whose activities could be abused for terrorist financing purposes?

Countries and geographical areas

22. When identifying the risk associated with countries and geographical areas, firms should consider the risk related to:

a) the jurisdictions in which the customer and beneficial owner are based;

b) the jurisdictions that are the customer's and beneficial owner's main places of business; and

c) the jurisdictions to which the customer and beneficial owner have relevant personal links.

23. Firms should note that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors (see also paragraphs 36-38). For example:

- Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant.

- Where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating, firms should consider to what extent this could be expected to or might give rise to suspicion, based on what the firm knows about the purpose and nature of the business relationship.

- Where the customer is a credit or financial institution, firms should pay particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision.

- Where the customer is a legal vehicle or trust, firms should take into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency standards.

24. Risk factors firms should consider when identifying the effectiveness of a jurisdiction's AML/CFT regime include:

- Has the country been identified by the Commission as having strategic deficiencies in its AML/CFT regime, in line with Article 9 of Directive (EU) 2015/849? Where firms

[7] See, in particular, Articles 1(7) and 16(4) of Directive 2014/92/EU.

deal with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, firms must always apply EDD measures.[8]

- Is there information from more than one credible and reliable source about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point is the executive summary and key findings and the assessment of compliance with Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports. Firms should note that membership of the FATF or an FSRB (e.g. MoneyVal) does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective.

Firms should note that Directive (EU) 2015/849 does not recognise the 'equivalence' of third countries and that EU Member States' lists of equivalent jurisdictions are no longer being maintained. To the extent permitted by national legislation, firms should be able to identify lower risk jurisdictions in line with these guidelines and Annex II of Directive (EU) 2015/849.

25. Risk factors firms should consider when identifying the level of terrorist financing risk associated with a jurisdiction include:

- Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?

- Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union ?

26. Risk factors firms should consider when identifying a jurisdiction's level of transparency and tax compliance include:

- Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting

[8] Article 18(1) of Directive (EU) 2015/849.

Standard; assessments of compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).

- Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?

- Has the jurisdiction put in place reliable and accessible beneficial ownership registers?

27. Risk factors firms should consider when identifying the risk associated with the level of predicate offences to money laundering include:

- Is there information from credible and reliable public sources about the level of predicate offences to money laundering listed in Article 3(4) of Directive (EU) 2015/849, for example corruption, organised crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.

- Is there information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectively to investigate and prosecute these offences?

Products, services and transactions risk factors

28. When identifying the risk associated with their products, services or transactions, firms should consider the risk related to:

a) the level of transparency, or opaqueness, the product, service or transaction affords;

b) the complexity of the product, service or transaction; and

c) the value or size of the product, service or transaction.

29. Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency include:

- To what extent do products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, offshore vehicles and certain trusts, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.

- To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?

30. Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

- To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions, for example in the case of certain trade finance transactions? Are transactions straightforward, for example are regular payments made into a pension fund?

- To what extent do products or services allow payments from third parties or accept overpayments where this is would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example is it a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under Directive (EU) 2015/849?

- Does the firm understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

31. Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size include:

- To what extent are products or services cash intensive, as are many payment services but also certain current accounts?

- To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?

Delivery channel risk factors

32. When identifying the risk associated with the way in which the customer obtains the products or services they require, firms should consider the risk related to:

a) the extent to which the business relationship is conducted on a non-face-to-face basis; and

b) any introducers or intermediaries the firm might use and the nature of their relationship with the firm.

33. When assessing the risk associated with the way in which the customer obtains the products or services, firms should consider a number of factors including:

- Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?

- Has the customer been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the

customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures to European Economic Area (EEA) standards in line with Article 28 of Directive (EU) 2015/849?

- Has the customer been introduced by a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:

  i. the third party applies CDD measures and keeps records to EEA standards and that it is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of Directive (EU) 2015/849;

  ii. the third party will provide, immediately upon request, relevant copies of identification and verification data, inter alia in line with Article 27 of Directive (EU) 2015/849; and

  iii. the quality of the third party's CDD measures is such that it can be relied upon?

- Has the customer been introduced through a tied agent, that is, without direct firm contact? To what extent can the firm be satisfied that the agent has obtained enough information so that the firm knows its customer and the level of risk associated with the business relationship?

- If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the firm's knowledge of the customer and ongoing risk management?

- Where a firm uses an intermediary:

  i. Are they a regulated person subject to AML obligations that are consistent with those of Directive (EU) 2015/849?

  ii. Are they subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example has the intermediary been sanctioned for breaches of AML/CFT obligations?

  iii. Are they based in a jurisdiction associated with higher ML/TF risk? Where a third party is based in a high-risk third country that the Commission has identified as having strategic deficiencies, firms must not rely on that intermediary. However, to the extent permitted by national legislation, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary of another firm established in the Union, and the firm is confident that the intermediary fully complies with group-wide policies

and procedures in line with Article 45 of Directive (EU) 2015/849.[9]

Assessing ML/TF risk

34. Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship or occasional transaction.

35. As part of this assessment, firms may decide to weigh factors differently depending on their relative importance.

Weighting risk factors

36. When weighting risk factors, firms should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction. This often results in firms allocating different 'scores' to different factors; for example, firms may decide that a customer's personal links to a jurisdiction associated with higher ML/TF risk is less relevant in light of the features of the product they seek.

37. Ultimately, the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another. When weighting risk factors, firms should ensure that:

- weighting is not unduly influenced by just one factor;
- economic or profit considerations do not influence the risk rating;
- weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- the provisions of Directive (EU) 2015/849 or national legislation regarding situations that always present a high money laundering risk cannot be over-ruled by the firm's weighting; and
- they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

38. Where a firm uses automated IT systems to allocate overall risk scores to categorise business relationships or occasional transactions and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. A firm must always be able to satisfy itself that the scores allocated reflect the firm's understanding of ML/TF risk and it should be able to demonstrate this to the competent authority.

[9] Article 26(2) of Directive (EU) 2015/849.

Categorising business relationships and occasional transactions

39. Following its risk assessment, a firm should categorise its business relationships and occasional transactions according to the perceived level of ML/TF risk.

40. Firms should decide on the most appropriate way to categorise risk. This will depend on the nature and size of the firm's business and the types of ML/TF risk it is exposed to. Although firms often categorise risk as high, medium and low, other categorisations are possible.

Risk management: simplified and enhanced customer due diligence

41. A firm's risk assessment should help it identify where it should focus its AML/CFT risk management efforts, both at customer take-on and for the duration of the business relationship.

42. As part of this, firms must apply each of the CDD measures set out in Article 13(1) of Directive (EU) 2015/849 but may determine the extent of these measures on a risk-sensitive basis. CDD measures should help firms better understand the risk associated with individual business relationships or occasional transactions.

43. Article 13(4) of Directive (EU) 2015/849 requires firms to be able to demonstrate to their competent authority that the CDD measures they have applied are commensurate to the ML/TF risks.

Simplified customer due diligence

44. To the extent permitted by national legislation, firms may apply SDD measures in situations where the ML/TF risk associated with a business relationship has been assessed as low. SDD is not an exemption from any of the CDD measures; however, firms may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they have identified.

45. SDD measures firms may apply include but are not limited to:

- adjusting the timing of CDD, for example where the product or transaction sought has features that limit its use for ML/TF purposes, for example by:

  i. verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or

  ii. verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. Firms must make sure that:

a) this does not result in a de facto exemption from CDD, that is, firms must ensure that the customer's or beneficial owner's identity will ultimately be verified;

b) the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, firms should note that a low threshold alone may not be enough to reduce risk);

c) they have systems in place to detect when the threshold or time limit has been reached; and

d) they do not defer CDD or delay obtaining relevant information about the customer where applicable legislation, for example Regulation (EU) 2015/847 or provisions in national legislation, require that this information be obtained at the outset.

- adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:

  i. verifying identity on the basis of information obtained from one reliable, credible and independent document or data source only; or

  ii. assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme or a shopping centre gift card.

- adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:

  i. accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity (note that this is not permitted in relation to the verification of the customer's identity); or

  ii. where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the CDD requirements, for example where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name at an EEA firm.

- adjusting the frequency of CDD updates and reviews of the business relationship, for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached; firms must make sure that this does not result in a *de facto* exemption from keeping CDD information up-to-date.

- adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where firms choose to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

46. Title III lists additional SDD measures that may be of particular relevance in different sectors.

47. The information a firm obtains when applying SDD measures must enable the firm to be reasonably satisfied that its assessment that the risk associated with the relationship is low is justified. It must also be sufficient to give the firm enough information about the nature of the business relationship to identify any unusual or suspicious transactions. SDD does not exempt an institution from reporting suspicious transactions to the FIU.

48. Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied.[10] Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

Enhanced customer due diligence

49. Firms must apply EDD measures in higher risk situations to manage and mitigate those risks appropriately.[11] EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures.

50. Directive (EU) 2015/849 lists specific cases that firms must always treat as high risk:

    i. where the customer, or the customer's beneficial owner, is a PEP;[12]

    ii. where a firm enters into a correspondent relationship with a respondent institution from a non-EEA state;[13]

    iii. where a firm deals with natural persons or legal entities established in high-risk third countries;[14] and

    iv. all complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.[15]

51. Directive (EU) 2015/849 sets out specific EDD measures that firms must apply:

    i. where the customer, or the customer's beneficial owner, is a PEP;

    ii. with respect to correspondent relationships with respondents from third countries; and

[10] Article 11(e) and (f) and Article 15(2) of Directive (EU) 2015/849.
[11] Articles 18-24 of Directive (EU) 2015/849.
[12] Articles 20-24 of Directive (EU) 2015/849.
[13] Article 19 of Directive (EU) 2015/849.
[14] Article 18(1) of Directive (EU) 2015/849.
[15] Article 18(2) of Directive (EU) 2015/849.

iii. with respect to all complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.

Firms should apply additional EDD measures in those situations where this is commensurate to the ML/TF risk they have identified.

Politically Exposed Persons

52. Firms that have identified that a customer or beneficial owner is a PEP must always:

- Take adequate measures to establish the source of wealth and the source of funds to be used in the business relationship in order to allow the firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures firms should take to establish the PEP's source of wealth and the source of funds will depend on the degree of high risk associated with the business relationship. Firms should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

- Obtain senior management approval for entering into, or continuing, a business relationship with a PEP. The appropriate level of seniority for sign-off should be determined by the level of increased risk associated with the business relationship, and the senior manager approving a PEP business relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the firm's risk profile.

  When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the firm would be exposed to if it entered into that business relationship and how well equipped the firm is to manage that risk effectively.

- Apply enhanced ongoing monitoring of both transactions and the risk associated with the business relationship. Firms should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of high risk associated with the relationship.

53. Firms must apply all of these measures to PEPs, their family members and known close associates and should adjust the extent of these measures on a risk-sensitive basis.[16]

Correspondent relationships

54. Firms must take specific EDD measures where they have a cross-border correspondent

[16] Article 20(b) of Directive (EU) 2015/849.

relationship with a respondent who is based in a third country.[17] Firms must apply all of these measures and should adjust the extent of these measures on a risk-sensitive basis.

55. Firms should refer to Title III for guidelines on EDD in relation to correspondent banking relationships; these guidelines may also be useful for firms in other correspondent relationships.

Unusual transactions

56. Firms should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where a firm detects transactions that are unusual because:

- they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;
- they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- they are very complex compared with other, similar, transactions associated with similar customer types, products or services,

and the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given, it must apply EDD measures.

57. These EDD measures should be sufficient to help the firm determine whether these transactions give rise to suspicion and must at least include:

- taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.

High-risk third countries and other high-risk situations

58. When dealing with natural persons or legal persons established or residing in a high-risk third country identified by the Commission[18] and in all other high-risk situations, firms should take an informed decision about which EDD measures are appropriate for each high-risk situation. The appropriate type of EDD, including the extent of the additional information sought, and of the increased monitoring carried out, will depend on the

[17] Article 19 of Directive (EU) 2015/849.

[18] Article 9 of Directive (EU) 2015/849.

reason why an occasional transaction or a business relationship was classified as high risk.

59. Firms are not required to apply all the EDD measures listed below in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship.

60. EDD measures firms should apply may include:

- Increasing the quantity of information obtained for CDD purposes:

  i. Information about the customer's or beneficial owner's identity, or the customer's ownership and control structure, to be satisfied that the risk associated with the relationship is well understood. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include:

     a. information about family members and close business partners;

     b. information about the customer's or beneficial owner's past and present business activities; and

     c. adverse media searches.

  ii. Information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete customer risk profile. This may include obtaining information on:

     a. the number, size and frequency of transactions that are likely to pass through the account, to enable the firm to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);

     b. why the customer is looking for a specific product or service, in particular where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;

     c. the destination of funds;

     d. the nature of the customer's or beneficial owner's business, to enable the firm to better understand the likely nature of the business relationship.

- Increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity including by:

  i. requiring the first payment to be carried out through an account verifiably in the customer's name with a bank subject to CDD standards that are not less robust than those set out in Chapter II of Directive (EU) 2015/849; or

ii. establishing that the customer's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the firm's knowledge of the customer and the nature of the business relationship. In some cases, where the risk associated with the relationship is particularly high, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports.

- Increasing the frequency of reviews to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship or conclude that the relationship no longer corresponds to the firm's risk appetite and to help identify any transactions that require further review, including by:

i. increasing the frequency of reviews of the business relationship to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;

ii. obtaining the approval of senior management to commence or continue the business relationship to ensure that senior management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

iii. reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and, where necessary, acted upon; or

iv. conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

61. Title III lists additional EDD measures that may be of particular relevance in different sectors.

Other considerations

62. Firms should not enter into a business relationship if they are unable to comply with their CDD requirements, if they are not satisfied that the purpose and nature of the business relationship are legitimate or if they are not satisfied that they can effectively manage the risk that they may be used for ML/TF purposes. Where such a business relationship already exists, firms should terminate it or suspend transactions until it can be terminated, subject to instructions from law enforcement, where applicable.

63. Where firms have reasonable grounds to suspect that ML/TF is being attempted, firms must report this to their FIU.

64. Firms should note that the application of a risk-based approach does not of itself require them to refuse, or terminate, business relationships with entire categories of customers

that they associate with higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one category.

Monitoring and review

Risk assessment

65. Firms should keep their assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure their assessment of ML/TF risk remains up to date and relevant. Firms should assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

66. Firms should also ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business-wide and individual risk assessments in a timely manner.

67. Examples of systems and controls firms should put in place to identify emerging risks include:

- Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues, in relation to both individual business relationships and the firm's business.

- Processes to ensure that the firm regularly reviews relevant information sources such as those specified in paragraphs 15 and 16 of these guidelines. This should involve, in particular:

  i. regularly reviewing media reports that are relevant to the sectors or jurisdictions in which the firm is active;

  ii. regularly reviewing law enforcement alerts and reports;

  iii. ensuring that the firm becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates; and

  iv. regularly reviewing thematic reviews and similar publications issued by competent authorities.

- Processes to capture and review information on risks relating to new products.

- Engagement with other industry representatives and competent authorities (e.g. round tables, conferences and training providers), and processes to feed back any findings to relevant staff.

- Establishing a culture of information sharing within the firm and strong company ethics.

68. Examples of systems and controls firms should put in place to ensure their individual and business-wide risk assessments remains up to date may include:

- Setting a date on which the next risk assessment update will take place, for example on 1 March every year, to ensure new or emerging risks are included in risk assessments. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in risk assessments as soon as possible.

- Carefully recording issues throughout the year that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

69. Like the original risk assessments, any update to a risk assessment and adjustment of accompanying CDD measures should be proportionate and commensurate to the ML/TF risk.

Systems and controls

70. Firms should take steps to ensure that their risk management systems and controls, in particular those relating to the application of the right level of CDD measures, are effective and proportionate.

Record keeping

71. Firms should record and document their risk assessments of business relationships, as well as any changes made to risk assessments as part of their reviews and monitoring, to ensure that they can demonstrate to the competent authorities that their risk assessments and associated risk management measures are adequate.

Title III – Sector-specific guidelines

72. The sector-specific guidelines in Title III complement the general guidance in Title II of these guidelines. They should be read in conjunction with Title II of these guidelines.

73. The risk factors described in each chapter of Title III are not exhaustive. Firms should take a holistic view of the risk associated with the situation and note that isolated risk factors do not necessarily move a business relationship or occasional transaction into a higher or lower risk category.

74. Each chapter in Title III also sets out examples of the CDD measures firms should apply on a risk-sensitive basis in high-risk and, to the extent permitted by national legislation, low-risk situations. These examples are not exhaustive and firms should decide on the most appropriate CDD measures in line with the level and type of ML/TF risk they have identified.

Chapter 1: Sectoral guidelines for correspondent banks

75. This chapter provides guidelines on correspondent banking as defined in Article 3(8)(a) of Directive (EU) 2015/849. Firms offering other correspondent relationships as defined in Article 3(8)(b) of Directive (EU) 2015/849 should apply these guidelines as appropriate.

76. In a correspondent banking relationship, the correspondent provides banking services to the respondent, either in a principal-to-principal capacity or on the respondent's customers' behalf. The correspondent does not normally have a business relationship with the respondent's customers and will not normally know their identity or the nature or purpose of the underlying transaction, unless this information is included in the payment instruction.

77. Banks should consider the following risk factors and measures alongside those set out in Title II of these guidelines.

Risk factors

Product, service and transaction risk factors

78. The following factors may contribute to increasing risk:

- The account can be used by other respondent banks that have a direct relationship with the respondent but not with the correspondent ('nesting', or downstream clearing), which means that the correspondent is indirectly providing services to other banks that are not the respondent.
- The account can be used by other entities within the respondent's group that have not themselves been subject to the correspondent's due diligence.
- The service includes the opening of a payable-through account, which allows the respondent's customers to carry out transactions directly on the account of the respondent.

79. The following factors may contribute to reducing risk:

- The relationship is limited to a SWIFT RMA capability, which is designed to manage communications between financial institutions. In a SWIFT RMA relationship, the respondent, or counterparty, does not have a payment account relationship.
- Banks are acting in a principal-to-principal capacity, rather than processing transactions on behalf of their underlying clients, for example in the case of foreign exchange services between two banks where the business is transacted on a principal-to-principal basis between the banks and where the settlement of a transaction does not involve a payment to a third party. In those cases, the transaction is for the own account of the respondent bank.
- The transaction relates to the selling, buying or pledging of securities on regulated markets, for example when acting as or using a custodian with direct access, usually

through a local participant, to an EU or non-EU securities settlement system.

Customer risk factors

80. The following factors may contribute to increasing risk:

- The respondent's AML/CFT policies and the systems and controls the respondent has in place to implement them fall short of the standards required by Directive (EU) 2015/849.
- The respondent is not subject to adequate AML/CFT supervision.
- The respondent, its parent or a firm belonging to the same group as the respondent has recently been the subject of regulatory enforcement for inadequate AML/CFT policies and procedures and/or breaches of AML/CFT obligations.
- The respondent conducts significant business with sectors that are associated with higher levels of ML/TF risk; for example, the respondent conducts significant remittance business or business on behalf of certain money remitters or exchange houses, with non-residents or in a currency other than that of the country in which it is based.
- The respondent's management or ownership includes PEPs, in particular where a PEP can exert meaningful influence over the respondent, where the PEP's reputation, integrity or suitability as a member of the management board or key function holder gives rise to concern or where the PEP is from a jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to those jurisdictions where corruption is perceived to be systemic or widespread.
- The history of the business relationship with the respondent gives rise to concern, for example because the amount of transactions are not in line with what the correspondent would expect based on its knowledge of the nature and size of the respondent.

81. The following factors may contribute to reducing risk:

The correspondent is satisfied that:

- the respondent's AML/CFT controls are not less robust than those required by Directive (EU) 2015/849;
- the respondent is part of the same group as the correspondent, is not based in a jurisdiction associated with higher ML/TF risk and complies effectively with group AML standards that are not less strict than those required by Directive (EU) 2015/849.

Country or geographical risk factors

82. The following factors may contribute to increasing risk:

- The respondent is based in a jurisdiction associated with higher ML/TF risk. Firms

should pay particular attention to those jurisdictions

- with significant levels of corruption and/or other predicate offences to money laundering;
- without adequate capacity of the legal and judicial system effectively to prosecute those offences; or
- without effective AML/CFT supervision.[19]

- The respondent conducts significant business with customers based in a jurisdiction associated with higher ML/TF risk.
- The respondent's parent is headquartered or is incorporated in a jurisdiction associated with higher ML/TF risk.

83. The following factors may contribute to reducing risk:

- The respondent is based in an EEA member country.
- The respondent is based in a third country that has AML/CFT requirements not less robust than those required by Directive (EU) 2015/849 and effectively implements those requirements (although correspondents should note that this does not exempt them from applying EDD measures set out in Article 19 of Directive (EU) 2015/849).

Measures

84. All correspondents must carry out CDD on the respondent, who is the correspondent's customer, on a risk-sensitive basis.[20] This means that correspondents must:

- Identify, and verify the identity of, the respondent and its beneficial owner. As part of this, correspondents should obtain sufficient information about the respondent's business and reputation to establish that the money-laundering risk associated with the respondent is not increased. In particular, correspondents should:

  i. obtain information about the respondent's management and consider the relevance, for financial crime prevention purposes, of any links the respondent's management or ownership might have to PEPs or other high-risk individuals; and

  ii. consider, on a risk-sensitive basis, whether obtaining information about the respondent's major business, the types of customers it attracts, and the quality of its AML systems and controls (including publicly available information about any recent regulatory or criminal sanctions for AML failings) would be appropriate. Where the respondent is a branch, subsidiary or affiliate, correspondents should also consider the status, reputation and AML controls of the parent.

[19] See also Title II, paragraphs 22-27.

[20] Article 13 of Directive (EU) 2015/849.

- Establish and document the nature and purpose of the service provided, as well as the responsibilities of each institution. This may include setting out, in writing, the scope of the relationship, which products and services will be supplied, and how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent).

- Monitor the business relationship, including transactions, to identify changes in the respondent's risk profile and detect unusual or suspicious behaviour, including activities that are not consistent with the purpose of the services provided or that are contrary to commitments that have been concluded between the correspondent and the respondent. Where the correspondent bank allows the respondent's customers direct access to accounts (e.g. payable-through accounts, or nested accounts), it should conduct enhanced ongoing monitoring of the business relationship. Due to the nature of correspondent banking, post-execution monitoring is the norm.

- Ensure that the CDD information they hold is up to date.

85. Correspondents must also establish that the respondent does not permit its accounts to be used by a shell bank,[21] in line with Article 24 of Directive (EU) 2015/849. This may include asking the respondent for confirmation that it does not deal with shell banks, having sight of relevant passages in the respondent's policies and procedures, or considering publicly available information, such as legal provisions that prohibit the servicing of shell banks.

86. In cases of cross-border correspondent relationships with respondent institutions from third countries, Article 19 of Directive (EU) 2015/849 requires that the correspondent also apply specific EDD measures in addition to the CDD measures set out in Article 13 of Directive (EU) 2015/849.

87. There is no requirement in Directive (EU) 2015/849 for correspondents to apply CDD measures to the respondent's individual customers.

88. Correspondents should bear in mind that CDD questionnaires provided by international organisations are not normally designed specifically to help correspondents comply with their obligations under Directive (EU) 2015/849. When considering whether to use these questionnaires, correspondents should assess whether they will be sufficient to allow them to comply with their obligations under Directive (EU) 2015/849 and should take additional steps where necessary.

Respondents based in non-EEA countries

89. Where the respondent is based in a third country, Article 19 of Directive (EU) 2015/849 requires correspondents to apply specific EDD measures in addition to the CDD measures set out in Article 13 of Directive (EU) 2015/849.

90. Correspondents must apply each of these EDD measures to respondents based in a non-

[21] Article 3(17) of Directive (EU) 2015/849.

EEA country, but correspondents can adjust the extent of these measures on a risk-sensitive basis. For example, if the correspondent is satisfied, based on adequate research, that the respondent is based in a third country that has an effective AML/CFT regime, supervised effectively for compliance with these requirements, and that there are no grounds to suspect that the respondent's AML policies and procedures are, or have recently been deemed, inadequate, then the assessment of the respondent's AML controls may not necessarily have to be carried out in full detail.

91. Correspondents should always adequately document their CDD and EDD measures and decision-making processes.

92. Article 19 of Directive (EU) 2015/849 requires correspondents to take risk-sensitive measures to:

- Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, in order to establish the extent to which the respondent's business exposes the correspondent to higher money-laundering risk. This should include taking steps to understand and risk-assess the nature of respondent's customer base and the type of activities that the respondent will transact through the correspondent account.

- Determine from publicly available information the reputation of the institution and the quality of supervision. This means that the correspondent should assess the extent to which the correspondent can take comfort from the fact that the respondent is adequately supervised for compliance with its AML obligations. A number of publicly available resources, for example FATF or FSAP assessments, which contain sections on effective supervision, may help correspondents establish this.

- Assess the respondent institution's AML/CFT controls. This implies that the correspondent should carry out a qualitative assessment of the respondent's AML/CFT control framework, not just obtain a copy of the respondent's AML policies and procedures. This assessment should be documented appropriately. In line with the risk-based approach, where the risk is especially high and in particular where the volume of correspondent banking transactions is substantive, the correspondent should consider on-site visits and/or sample testing to be satisfied that the respondent's AML policies and procedures are implemented effectively.

- Obtain approval from senior management, as defined in Article 3(12) of Directive (EU) 2015/849, before establishing new correspondent relationships. The approving senior manager should not be the officer sponsoring the relationship and the higher the risk associated with the relationship, the more senior the approving senior manager should be. Correspondents should keep senior management informed of high-risk correspondent banking relationships and the steps the correspondent takes to manage that risk effectively.

- Document the responsibilities of each institution. This may be part of the correspondent's standard terms and conditions but correspondents should set out, in writing, how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent) and what the

respondent's AML/CFT responsibilities are. Where the risk associated with the relationship is high, it may be appropriate for the correspondent to satisfy itself that the respondent complies with its responsibilities under this agreement, for example through ex post transaction monitoring.

- With respect to payable-through accounts and nested accounts, be satisfied that the respondent credit or financial institution has verified the identity of and performed ongoing due diligence on the customer having direct access to accounts of the correspondent and that it is able to provide relevant CDD data to the correspondent institution upon request. Correspondents should seek to obtain confirmation from the respondent that the relevant data can be provided upon request.

Respondents based in EEA countries

93. Where the respondent is based in an EEA country, Article 19 of Directive (EU) 2015/849 does not apply. The correspondent is, however, still obliged to apply risk-sensitive CDD measures pursuant to Article 13 of Directive (EU) 2015/849.

94. Where the risk associated with a respondent based in an EEA Member State is increased, correspondents must apply EDD measures in line with Article 18 of Directive (EU) 2015/849. In that case, correspondents should consider applying at least some of the EDD measures described in Article 19 of Directive (EU) 2015/849, in particular Article 19(a) and (b).

Chapter 2: Sectoral guidelines for retail banks

95. For the purpose of these guidelines, retail banking means the provision of banking services to natural persons and small and medium-sized enterprises. Examples of retail banking products and services include current accounts, mortgages, savings accounts, consumer and term loans, and credit lines.

96. Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and business relationships, retail banking is vulnerable to terrorist financing and to all stages of the money laundering process. At the same time, the volume of business relationships and transactions associated with retail banking can make identifying ML/TF risk associated with individual relationships and spotting suspicious transactions particularly challenging.

97. Banks should consider the following risk factors and measures alongside those set out in Title II of these guidelines.

Risk factors

Product, service and transaction risk factors

98. The following factors may contribute to increasing risk:

- the product's features favour anonymity;
- the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected, for example for mortgages or loans;
- the product places no restrictions on turnover, cross-border transactions or similar product features;
- new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products where these are not yet well understood;
- lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;
- an unusually high volume or large value of transactions.

99. The following factors may contribute to reducing risk:

- The product has limited functionality, for example in the case of:
  i. a fixed term savings product with low savings thresholds;

ii. a product where the benefits cannot be realised for the benefit of a third party;

iii. a product where the benefits are only realisable in the long term or for a specific purpose, such as retirement or a property purchase;

iv. a low-value loan facility, including one that is conditional on the purchase of a specific consumer good or service; or

v. a low-value product, including a lease, where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated or is never passed at all.

- The product can only be held by certain categories of customers, for example pensioners, parents on behalf of their children, or minors until they reach the age of majority.

- Transactions must be carried out through an account in the customer's name at a credit or financial institution that is subject to AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

- There is no overpayment facility.

Customer risk factors

100. The following factors may contribute to increasing risk:

- The nature of the customer, for example:

i. The customer is a cash-intensive undertaking.

ii. The customer is an undertaking associated with higher levels of money laundering risk, for example certain money remitters and gambling businesses.

iii. The customer is an undertaking associated with a higher corruption risk, for example operating in the extractive industries or the arms trade.

iv. The customer is a non-profit organisation that supports jurisdictions associated with an increased TF risk

v. The customer is a new undertaking without an adequate business profile or track record.

vi. The customer is a non-resident. Banks should note that Article 16 of Directive 2014/92/EU creates a right for consumers who are legally resident in the European Union to obtain a basic bank account, although the right to open and use a basic payment account applies only to the extent that banks can comply with their AML/CFT obligations and does not exempt banks from their obligation

to identify and assess ML/TF risk, including the risk associated with the customer not being a resident of the Member State in which the bank is based.[22]

vii. The customer's beneficial owner cannot easily be identified, for example because the customer's ownership structure is unusual, unduly complex or opaque, or because the customer issues bearer shares.

- The customer's behaviour, for example:

i. The customer is reluctant to provide CDD information or appears deliberately to avoid face-to-face contact.

ii. The customer's evidence of identity is in a non-standard form for no apparent reason.

iii. The customer's behaviour or transaction volume is not in line with that expected from the category of customer to which they belong, or is unexpected based on the information the customer provided at account opening.

iv. The customer's behaviour is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, by means either of lump sum repayments or early termination; deposits or demands payout of high-value bank notes without apparent reason; increases activity after a period of dormancy; or makes transactions that appear to have no economic rationale.

101. The following factor may contribute to reducing risk:

- The customer is a long-standing client whose previous transactions have not given rise to suspicion or concern, and the product or service sought is in line with the customer's risk profile.

Country or geographical risk factors[23]

102. The following factors may contribute to increasing risk:

- The customer's funds are derived from personal or business links to jurisdictions associated with higher ML/TF risk.

- The payee is located in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

[22] See the EBA's 'Opinion on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories': http://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf .

[23] See also Title II.

103. The following factor may contribute to reducing risk:

- Countries associated with the transaction have an AML/CFT regime that is not less robust than that required under Directive (EU) 2015/849 and are associated with low levels of predicate offences.

Distribution channel risk factors

104. The following factors may contribute to increasing risk:

- non-face-to-face business relationships, where no adequate additional safeguards – for example electronic signatures, electronic identification certificates issued in accordance with Regulation EU (No) 910/2014 and anti-impersonation fraud checks – are in place;
- reliance on a third party's CDD measures in situations where the bank does not have a long-standing relationship with the referring third party;
- new delivery channels that have not been tested yet.

105. The following factor may contribute to reducing risk:

- The product is available only to customers who meet specific eligibility criteria set out by national public authorities, as in the case of state benefit recipients or specific savings products for children registered in a particular Member State.

Measures

106. Where banks use automated systems to identify ML/TF risk associated with individual business relationships or occasional transactions and to identify suspicious transactions, they should ensure that these systems are fit for purpose in line with the criteria set out in Title II. The use of automated IT systems should never be considered a substitute for staff vigilance.

Enhanced customer due diligence

107. Where the risk associated with a business relationship or occasional transaction is increased, banks must apply EDD measures.[24] These may include:

- Verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source.
- Identifying, and verifying the identity of, other shareholders who are not the customer's beneficial owner or any natural persons who have authority to operate an account or give instructions concerning the transfer of funds or the transfer of securities.

[24] Article 18 of Directive (EU) 2015/849.

- Obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile, for example by carrying out open source or adverse media searches or commissioning a third party intelligence report. Examples of the type of information banks may seek include:

  i. the nature of the customer's business or employment;

  ii. the source of the customer's wealth and the source of the customer's funds that are involved in the business relationship, to be reasonably satisfied that these are legitimate;

  iii. the purpose of the transaction, including, where appropriate, the destination of the customer's funds;

  iv. information on any associations the customer might have with other jurisdictions (headquarters, operating facilities, branches, etc.) and the individuals who may influence its operations; or

  v. where the customer is based in another country, why they seek retail banking services outside their home jurisdiction.

- Increasing the frequency of transaction monitoring.

- Reviewing and, where necessary, updating information and documentation held more frequently. Where the risk associated with the relationship is particularly high, banks should review the business relationship annually.

Simplified customer due diligence

108. In low-risk situations, and to the extent permitted by national legislation, banks may apply SDD measures, which may include:

- for customers that are subject to a statutory licensing and regulatory regime, verifying identity based on evidence of the customer being subject to that regime, for example through a search of the regulator's public register;

- verifying the customer's and, where applicable, the beneficial owner's identities during the establishment of the business relationship in accordance with Article 14(2) of Directive (EU) 2015/849;

- assuming that a payment drawn on an account in the sole or joint name of the customer at a regulated credit or financial institution in an EEA country satisfies the requirements stipulated by Article 13(1)(a) and (b) of Directive (EU) 2015/849;

- accepting alternative forms of identity that meet the independent and reliable source criterion in Article 13(1)(a) of Directive (EU) 2015/849, such as a letter from a government agency or other reliable public body to the customer, where there are reasonable grounds for the customer not to be able to provide standard evidence of identity and provided that there are no grounds for suspicion;

- updating CDD information only in case of specific trigger events, such as the customer requesting a new or higher risk product, or changes in the customer's behaviour or transaction profile that suggest that the risk associated with the relationship is no longer low.

Pooled accounts

109. Where a bank's customer opens a 'pooled account' in order to administer funds that belong to the customer's own clients, the bank should apply full CDD measures, including treating the customer's clients as the beneficial owners of funds held in the pooled account and verifying their identities.

110. Where there are indications that the risk associated with the business relationship is high, banks must apply EDD measures as appropriate.[25]

111. However, to the extent permitted by national legislation, where the risk associated with the business relationship is low and subject to the conditions set out below, a bank may apply SDD measures provided that:

- The customer is a firm that is subject to AML/CFT obligations in an EEA state or a third country with an AML/CFT regime that is not less robust than that required by Directive (EU) 2015/849, and is supervised effectively for compliance with these requirements.

- The customer is not a firm but another obliged entity that is subject to AML/CFT obligations in an EEA state and is supervised effectively for compliance with these requirements.

- The ML/TF risk associated with the business relationship is low, based on the bank's assessment of its customer's business, the types of clients the customer's business serves and the jurisdictions the customer's business is exposed to, among other considerations;

- the bank is satisfied that the customer applies robust and risk-sensitive CDD measures to its own clients and its clients' beneficial owners (it may be appropriate for the bank to take risk-sensitive measures to assess the adequacy of its customer's CDD policies and procedures, for example by liaising directly with the customer); and

- the bank has taken risk-sensitive steps to be satisfied that the customer will provide CDD information and documents on its underlying clients that are the beneficial owners of funds held in the pooled account immediately upon request, for example by including relevant provisions in a contract with the customer or by sample-testing the customer's ability to provide CDD information upon request.

112. Where the conditions for the application of SDD to pooled accounts are met, SDD measures may consist of the bank:

[25] Articles 13(1) and 18(1) of Directive (EU) 2015/849.

- identifying and verifying the identity of the customer, including the customer's beneficial owners (but not the customer's underlying clients);
- assessing the purpose and intended nature of the business relationship; and
- conducting ongoing monitoring of the business relationship.

Chapter 3: Sectoral guidelines for electronic money issuers

113. This chapter provides guidelines for electronic money issuers (e-money issuers) as defined in Article 2(3) of Directive 2009/110/EC. The level of ML/TF risk associated with electronic money[26] (e-money) depends primarily on the features of individual e-money products and the degree to which e-money issuers use other persons to distribute and redeem e-money on their behalf.[27]

114. Firms that issue e-money should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines for money remitters in Title III, Chapter 4, may also be relevant in this context.

Risk factors

Product risk factors

115. E-money issuers should consider the ML/TF risk related to:

- thresholds;
- the funding method; and
- utility and negotiability.

116. The following factors may contribute to increasing risk:

- Thresholds: the product allows
  i. high-value or unlimited-value payments, loading or redemption, including cash withdrawal;
  ii. high-value payments, loading or redemption, including cash withdrawal;
  iii. high or unlimited amount of funds to be stored on the e-money product/account.
- Funding method: the product can be
  i. loaded anonymously, for example with cash, anonymous e-money or e-money products that benefit from the exemption in Article 12 of Directive (EU) 2015/849;
  ii. funded with payments from unidentified third parties;
  iii. funded with other e-money products.

[26] Article 2(2) of Directive 2009/110/EC.
[27] Article 3(4) of Directive 2009/110/EC.

- Utility and negotiability: the product

  i. allows person-to-person transfers;

  ii. is accepted as a means of payment by a large number of merchants or points of sale;

  iii. is designed specifically to be accepted as a means of payment by merchants dealing in goods and services associated with a high risk of financial crime, for example online gambling;

  iv. can be used in cross-border transactions or in different jurisdictions;

  v. is designed to be used by persons other than the customer, for example certain partner card products (but not low-value gift cards);

  vi. allows high-value cash withdrawals.

117. The following factors may contribute to reducing risk:

- Thresholds: the product

  i. sets low-value limits on payments, loading or redemption, including cash withdrawal (although firms should note that a low threshold alone may not be enough to reduce TF risk);

  ii. limits number of payments, loading or redemption, including cash withdrawal in a given period;

  iii. limits the amount of funds that can be stored on the e-money product/account at any one time.

- Funding: the product

  i. requires that the funds for purchase or reloading are verifiably drawn from an account held in the customer's sole or joint name at an EEA credit or financial institution;

- Utility and negotiability: the product

  i. does not allow or strictly limits cash withdrawal;

  ii. can be used only domestically;

  iii. is accepted by a limited number of merchants or points of sale, with whose business the e-money issuer is familiar;

  iv. is designed specifically to restrict its use by merchants dealing in goods and services that are associated with a high risk of financial crime;

v. is accepted as a means of payment for limited types of low-risk services or products.

Customer risk factors

118. The following factors may contribute to increasing risk:

- The customer purchases several e-money products from the same issuer, frequently reloads the product or make several cash withdrawals in a short period of time and without an economic rationale; where distributors (or agents acting as distributors) are obliged entities themselves, this also applies to e-money products from different issuers purchased from the same distributor.

- The customer's transactions are always just below any value/transaction limits.

- The product appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from several IP addresses at the same time).

- There are frequent changes in the customer's identification data, such as home address or IP address, or linked bank accounts.

- The product is not used for the purpose it was designed for, for example it is used overseas when it was designed as a shopping centre gift card.

119. The following factor may contribute to reducing risk:

- The product is available only to certain categories of customers, for example social benefit recipients or members of staff of a company that issues them to cover corporate expenses.

Distribution channel risk factors

120. The following factors may contribute to increasing risk:

- Online and non-face-to-face distribution without adequate safeguards, such as electronic signatures, electronic identification documents meeting the criteria set out in Regulation (EU) No 910/2014 and anti-impersonation fraud measures.

- Distribution through intermediaries that are not themselves obliged entities under Directive (EU) 2015/849 or national legislation where applicable, where the e-money issuer:

  i. relies on the intermediary to carry out some of the AML/CFT obligations of the e-money issuer; and

  ii. has not satisfied itself that the intermediary has in place adequate AML/CFT systems and controls.

- Segmentation of services, that is, the provision of e-money services by several operationally independent service providers without due oversight and coordination.

Country or geographical risk factors;[28]

121. The following factors may contribute to increasing risk:

- The payee is located in, or the product receives funds from sources in, a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

Measures

122. National legislation may provide for an exemption from identification and verification of the customer's and beneficial owners' identities and assessment of the nature and purpose of the business relationship for certain E-money products in accordance with Article 12 of Directive (EU) 2015/849.

123. Firms should note that the exemption under Article 12 of Directive (EU) 2015/849 does not extend to the obligation to conduct ongoing monitoring of transactions and the business relationship, nor does it exempt them from the obligation to identify and report suspicious transactions; this means that firms should ensure that they obtain sufficient information about their customers, or the types of customers their product will target, to be able to carry out meaningful ongoing monitoring of the business relationship.

124. Examples of the types of monitoring systems firms should put in place include:

- transaction monitoring systems that detect anomalies or suspicious patterns of behaviour, including the unexpected use of the product in a way for which it was not designed; the firm may be able to disable the product either manually or through on-chip controls until it has been able to satisfy itself that there are no grounds for suspicion;

- systems that identify discrepancies between submitted and detected information, for example, between submitted country of origin information and the electronically detected IP address;

- systems that compare data submitted with data held on other business relationships and that can identify patterns such as the same funding instrument or the same contact details;

- systems that identify whether the product is used with merchants dealing in goods and services that are associated with a high risk of financial crime.

[28] See Title II, paragraphs 22-27.

Enhanced customer due diligence

125. Examples of EDD measures firms should apply in a high-risk situation include:

- obtaining additional customer information during identification, such as the source of funds;
- applying additional verification measures from a wider variety of reliable and independent sources (e.g. checking against online databases) in order to verify the customer's or beneficial owner's identity;
- obtaining additional information about the intended nature of the business relationship, for example by asking customers about their business or the jurisdictions to which they intend to transfer E-money;
- obtaining information about the merchant/payee, in particular where the E-money issuer has grounds to suspect that its products are being used to purchase illicit or age-restricted goods;
- applying identity fraud checks to ensure that the customer is who they claim to be;
- applying enhanced monitoring to the customer relationship and individual transactions;
- establishing the source and/or the destination of funds.

Simplified customer due diligence

126. To the extent permitted by national legislation, firms may consider applying SDD to low-risk e-money products that do not benefit from the exemption provided by Article 12 of Directive (EU) 2015/849.

127. To the extent permitted by national legislation, examples of SDD measures firms may apply in low-risk situations include:

- postponing the verification of the customer's or beneficial owner's identity to a certain later date after the establishment of the relationship or until a certain (low) monetary threshold is exceeded (whichever occurs first). The monetary threshold should not exceed EUR 250 where the product is not reloadable or can be used in other jurisdictions or for cross-border transactions or EUR 500 where permitted by national legislation (in this case, the product can be used only domestically);
- verifying the customer's identity on the basis of a payment drawn on an account in the sole or joint name of the customer or an account over which the customer can be shown to have control with an EEA-regulated credit or financial institution;
- verifying identity on the basis of fewer sources;
- verifying identity on the basis of less reliable sources;

- using alternative methods to verify identity;

- assuming the nature and intended purpose of the business relationship where this is obvious, for example in the case of certain gift cards that do not fall under the closed loop/closed network exemption;

- reducing the intensity of monitoring as long as a certain monetary threshold is not reached. As ongoing monitoring is an important means of obtaining more information on customer risk factors (see above) during the course of a customer relationship, that threshold for both individual transactions and transactions that appear to be linked over the course of 12 months should be set at a level that the firm has assessed as presenting a low risk for both terrorist financing and money laundering purposes.

Chapter 4: Sectoral guidelines for money remitters

128. Money remitters are payment institutions that have been authorised in line with Directive 2007/64/EC to provide and execute payment services throughout the EU. The businesses in this sector are diverse and range from individual businesses to complex chain operators.

129. Many money remitters use agents to provide payment services on their behalf. Agents often provide payment services as an ancillary component to their main business and they may not themselves be obliged entities under applicable AML/CFT legislation; accordingly, their AML/CFT expertise may be limited.

130. The nature of the service provided can expose money remitters to ML/TF risk. This is due to the simplicity and speed of transactions, their worldwide reach and their often cash-based character. Furthermore, the nature of this payment service means that money remitters often carry out occasional transactions rather than establishing a business relationship with their customers, which means that their understanding of the ML/TF risk associated with the customer may be limited.

131. Money remitters should consider the following risk factors and measures alongside those set out in Title II of these guidelines.

Risk factors

Product, service and transaction risk factors

132. The following factors may contribute to increasing risk:

- the product allows high-value or unlimited-value transactions;
- the product or service has a global reach;
- the transaction is cash-based or funded with anonymous electronic money, including electronic money benefiting from the exemption under Article 12 of Directive (EU) 2015/849;
- transfers are made from one or more payers in different countries to a local payee.

133. The following factor may contribute to reducing risk:

- the funds used in the transfer come from an account held in the payer's name at an EEA credit or financial institution

Customer risk factors

134. The following factors may contribute to increasing risk:

- The customer's business activity:

i. The customer owns or operates a business that handles large amounts of cash.

ii. The customer's business has a complicated ownership structure.

- The customer's behaviour:

i. The customer's needs may be better serviced elsewhere, for example because the money remitter is not local to the customer or the customer's business.

ii. The customer appears to be acting for someone else, for example others watch over the customer or are visible outside the place where the transaction is made, or the customer reads instructions from a note.

iii. The customer's behaviour makes no apparent economic sense, for example the customer accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency that is not official tender or commonly used in the jurisdiction where the customer and/or recipient is located or requests or provides large amounts of currency in either low or high denominations.

iv. The customer's transactions are always just below applicable thresholds, including the CDD threshold for occasional transactions in Article 11(b) of Directive (EU) 2015/849 and the EUR 1 000 threshold specified in Article 5(2) of Regulation (EU) 2015/847.[29] Firms should note that the threshold in Article 5(2) of Regulation (EU) 2015/847 applies only to transactions that are not funded by cash or anonymous electronic money.

v. The customer's use of the service is unusual, for example they send or receive money to or from themselves or send funds on immediately after receiving them.

vi. The customer appears to know little or is reluctant to provide information about the payee.

vii. Several of the firm's customers transfer funds to the same payee or appear to have the same identification information, for example address or telephone number.

viii. An incoming transaction is not accompanied by the required information on the payer or payee.

ix. The amount sent or received is at odds with the customer's income (if known).

135. The following factors may contribute to reducing risk:

- The customer is a long-standing customer of the firm whose past behaviour has not given rise to suspicion and there are no indications that the ML/TF risk might be

[29] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance).

increased.

- The amount transferred is low; however, firms should note that low amounts alone will not be enough to discount TF risk.

Distribution channel risk factors

136. The following factors may contribute to increasing risk:

- There are no restrictions on the funding instrument, for example in the case of cash or payments from E-money products that benefit from the exemption in Article 12 of Directive (EU) 2015/849, wire transfers or cheques.
- The distribution channel used provides a degree of anonymity.
- The service is provided entirely online without adequate safeguards.
- The money remittance service is provided through agents that:
  i. represent more than one principal;
  ii. have unusual turnover patterns compared with other agents in similar locations, for example unusually high or low transaction sizes, unusually large cash transactions or a high number of transactions that fall just under the CDD threshold, or undertake business outside normal business hours;
  iii. undertake a large proportion of business with payers or payees from jurisdictions associated with higher ML/TF risk;
  iv. appear to be unsure about, or inconsistent in, the application of group-wide AML/CFT policies; or
  v. are not from the financial sector and conduct another business as their main business.
- The money remittance service is provided through a large network of agents in different jurisdictions.
- The money remittance service is provided through an overly complex payment chain, for example with a large number of intermediaries operating in different jurisdictions or allowing for untraceable (formal and informal) settlement systems.

137. The following factors may contribute to reducing risk:

- Agents are themselves regulated financial institutions.
- The service can be funded only by transfers from an account held in the customer's name at an EEA credit or financial institution or an account over which the customer can be shown to have control.

Country or geographical risk factors

138. The following factors may contribute to increasing risk:

- The payer or the payee is located in a jurisdiction associated with higher ML/TF risk.
- The payee is resident in a jurisdiction that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used at point of payment.

Measures

139. Since many money remitters' business is primarily transaction-based, firms should consider which monitoring systems and controls they put in place to ensure that they detect money-laundering and terrorist financing attempts even where the CDD information they hold on the customer is basic or missing because no business relationship has been established.

140. Firms should in any case put in place:

- systems to identify linked transactions;
- systems to identify whether transactions from different customers are destined for the same payee;
- systems to permit as far as possible the establishment of the source of funds and the destination of funds;
- systems that allow the full traceability of both transactions and the number of operators included in the payment chain; and
- systems to ensure that throughout the payment chain only those duly authorised to provide money remittance services can intervene.

141. Where the risk associated with an occasional transaction or business relationship is increased, firms should apply EDD in line with Title II, including, where appropriate, increased transaction monitoring (e.g. increased frequency or lower thresholds). Conversely, where the risk associated with an occasional transaction or business relationship is low and to the extent permitted by national legislation, firms may be able to apply SDD measures in line with Title II.

Use of agents

142. Money remitters using agents to provide payment services should know who their agents are.[30] As part of this, money remitters should establish and maintain appropriate and risk-sensitive policies and procedures to counter the risk that their agents may engage in, or be used for, ML/TF, including by:

[30] Article 19 of Directive (EU) 2366/2015.

- Identifying the person who owns or controls the agent where the agent is a legal person, to be satisfied that the ML/TF risk to which the money remitter is exposed as a result of its use of the agent is not increased.

- Obtaining evidence, in line with the requirements of Article 19(1)(c) of Directive (EU) 2015/2366, that the directors and other persons responsible for the management of the agent are fit and proper persons, including by considering their honesty, integrity and reputation. Any enquiry the money remitter makes should be proportionate to the nature, complexity and scale of the ML/TF risk inherent in the payment services provided by the agent and could be based on the money remitter's CDD procedures.

- Taking reasonable measures to satisfy themselves that the agent's AML/CFT internal controls are appropriate and remain appropriate throughout the agency relationship, for example by monitoring a sample of the agent's transactions or reviewing the agent's controls on site. Where an agent's internal AML/CFT controls differ from the money remitter's, for example because the agent represents more than one principal or because the agent is itself an obliged entity under applicable AML/CFT legislation, the money remitter should assess and manage the risk that these differences might affect its own, and the agent's, AML/CFT compliance.

- Providing AML/CFT training to agents to ensure that agents have an adequate understanding of relevant ML/TF risks and the quality of the AML/CFT controls the money remitter expects.

Chapter 5: Sectoral guidelines for wealth management

143. Wealth management is the provision of banking and other financial services to high-net-worth individuals and their families or businesses. It is also known as private banking. Clients of wealth management firms can expect dedicated relationship management staff to provide tailored services covering, for example, banking (e.g. current accounts, mortgages and foreign exchange), investment management and advice, fiduciary services, safe custody, insurance, family office services, tax and estate planning and associated facilities, including legal support.

144. Many of the features typically associated with wealth management, such as wealthy and influential clients; very high-value transactions and portfolios; complex products and services, including tailored investment products; and an expectation of confidentiality and discretion are indicative of a higher risk for money laundering relative to those typically present in retail banking. Wealth management firms' services may be particularly vulnerable to abuse by clients who wish to conceal the origins of their funds or, for example, evade tax in their home jurisdiction.

145. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapters 2, 7 and 9, may also be relevant in this context.

Risk factors

Product, service and transaction risk factors

146. The following factors may contribute to increasing risk:

- customers requesting large amounts of cash or other physical stores of value such as precious metals;
- very high-value transactions;
- financial arrangements involving jurisdictions associated with higher ML/TF risk (firms should pay particular attention to countries that have a culture of banking secrecy or that do not comply with international tax transparency standards);[31]
- lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;
- the use of complex business structures such as trusts and private investment vehicles, particularly where the identity of the ultimate beneficial owner may be unclear;
- business taking place across multiple countries, particularly where it involves multiple

[31] See also Title II, paragraph 26.

providers of financial services;

- cross-border arrangements where assets are deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly where the other financial institution is based in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions with higher levels of predicate offences, a weak AML/CFT regime or weak tax transparency standards.

Customer risk factors

147. The following factors may contribute to increasing risk:

- Customers with income and/or wealth from high-risk sectors such as arms, the extractive industries, construction, gambling or private military contractors.
- Customers about whom credible allegations of wrongdoing have been made.
- Customers who expect unusually high levels of confidentiality or discretion.
- Customers whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behaviour.
- Very wealthy and influential clients, including customers with a high public profile, non-resident customers and PEPs. Where a customer or a customer's beneficial owner is a PEP, firms must always apply EDD in line with Articles 18 to 22 of Directive (EU) 2015/849.
- The customer requests that the firm facilitates the customer being provided with a product or service by a third party without a clear business or economic rationale.

Country or geographical risk factors[32]

148. The following factors may contribute to increasing risk:

- Business is conducted in countries that have a culture of banking secrecy or do not comply with international tax transparency standards.
- The customer lives in, or their funds derive from activity in, a jurisdiction associated with higher ML/TF risk.

Measures

149. The staff member managing a wealth management firm's relationship with a customer (the relationship manager) should play a key role in assessing risk. The relationship

[32] See also Title II.

manager's close contact with the customer will facilitate the collection of information that allows a fuller picture of the purpose and nature of the customer's business to be formed (e.g. an understanding of the client's source of wealth, why complex or unusual arrangements may nonetheless be genuine and legitimate, or why extra security may be appropriate). This close contact may, however, also lead to conflicts of interest if the relationship manager becomes too close to the customer, to the detriment of the firm's efforts to manage the risk of financial crime. Consequently, independent oversight of risk assessment will also be appropriate, provided by, for example, the compliance department and senior management.

Enhanced customer due diligence

150. The following EDD measures may be appropriate in high-risk situations:

- Obtaining and verifying more information about clients than in standard risk situations and reviewing and updating this information both on a regular basis and when prompted by material changes to a client's profile. Firms should perform reviews on a risk-sensitive basis, reviewing higher risk clients at least annually but more frequently if risk dictates. These procedures may include those for recording any visits to clients' premises, whether at their home or business, including any changes to client profile or other information that may affect risk assessment that these visits prompt.

- Establishing the source of wealth and funds; where the risk is particularly high and/or where the firm has doubts about the legitimate origin of the funds, verifying the source of wealth and funds may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, by reference to, inter alia:

  i. an original or certified copy of a recent pay slip;

  ii. written confirmation of annual salary signed by an employer;

  iii. an original or certified copy of contract of sale of, for example, investments or a company;

  iv. written confirmation of sale signed by an advocate or solicitor;

  v. an original or certified copy of a will or grant of probate;

  vi. written confirmation of inheritance signed by an advocate, solicitor, trustee or executor;

  vii. an internet search of a company registry to confirm the sale of a company.

- Establishing the destination of funds.

- Performing greater levels of scrutiny and due diligence on business relationships than would be typical in mainstream financial service provision, such as in retail banking or investment management.

- Carrying out an independent internal review and, where appropriate, seeking senior management approval of new clients and existing clients on a risk-sensitive basis.

- Monitoring transactions on an ongoing basis, including, where necessary, reviewing each transaction as it occurs, to detect unusual or suspicious activity. This may include measures to determine whether any of the following are out of line with the business risk profile:

  i. transfers (of cash, investments or other assets);

  ii. the use of wire transfers;

  iii. significant changes in activity;

  iv. transactions involving jurisdictions associated with higher ML/TF risk.

  Monitoring measures may include the use of thresholds, and an appropriate review process by which unusual behaviours are promptly reviewed by relationship management staff or (at certain thresholds) the compliance functions or senior management.

- Monitoring public reports or other sources of intelligence to identify information that relates to clients or to their known associates, businesses to which they are connected, potential corporate acquisition targets or third party beneficiaries to whom the client makes payments.

- Ensuring that cash or other physical stores of value (e.g. travellers' cheques) are handled only at bank counters, and never by relationship managers.

- Ensuring that the firm is satisfied that a client's use of complex business structures such as trusts and private investment vehicles is for legitimate and genuine purposes, and that the identity of the ultimate beneficial owner is understood.

Simplified customer due diligence

151. Simplified due diligence is not appropriate in a wealth management context.

Chapter 6: Sectoral guidelines for trade finance providers

152. Trade finance means managing a payment to facilitate the movement of goods (and the provision of services) either domestically or across borders. When goods are shipped internationally, the importer faces the risk that the goods will not arrive, while the exporter may be concerned that payment will not be forthcoming. To lessen these dangers, many trade finance instruments therefore place banks in the middle of the transaction.

153. Trade finance can take many different forms. These include:

- 'Open account' transactions: these are transactions where the buyer makes a payment once they have received the goods. These are the most common means of financing trade, but the underlying trade-related nature of the transaction will often not be known to the banks executing the fund transfer. Banks should refer to the guidance in Title II to manage the risk associated with such transactions.

- Documentary letters of credit (LCs): an LC is a financial instrument issued by a bank that guarantees payment to a named beneficiary (typically an exporter) upon presentation of certain 'complying' documents specified in the credit terms (e.g. evidence that goods have been dispatched).

- Documentary bills for collection (BCs): a BC refers to a process by which payment, or an accepted draft, is collected by a 'collecting' bank from an importer of goods for onward payment to the exporter. The collecting bank gives the relevant trade documentation (which will have been received from the exporter, normally through their bank) to the importer in return.

154. Other trade finance products such as forfaiting or structured financing, or wider activity such as project finance, are outside the scope of these sectoral guidelines. Banks offering these products should refer to the general guidance in Title II.

155. Trade finance products can be abused for money-laundering or terrorist financing purposes. For example, the buyer and seller may collude to misrepresent the price, type, quality or quantity of goods in order to transfer funds or value between countries.

156. The International Chamber of Commerce (ICC) has developed standards that govern the use of LCs and BCs, but these do not cover matters related to financial crime.33 Banks should note that these standards do not have legal force and their use does not mean that banks do not need to comply with their legal and regulatory AML/CFT obligations.

157. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapter 1, may also be relevant in this context.

[33] Uniform Customs and Practice for Documentary Credits (UCP 600) for LCs and Uniform Rules for Collections (URC 522) for BCs.

Risk factors

158. Banks party to trade finance transactions often have access only to partial information about the transaction and the parties to it. Trade documentation can be diverse and banks may not have expert knowledge of the different types of trade documentation they receive. This can make the identification and assessment of ML/TF risk challenging.

159. Banks should, nevertheless, use common sense and professional judgement to assess the extent to which the information and documentation they have could give rise to concern or suspicion of ML/TF.

160. To the extent possible, banks should consider the following risk factors:

Transaction risk factors

161. The following factors may contribute to increasing risk:

- The transaction is unusually large given what is known about a customer's previous trading activity.
- The transaction is highly structured, fragmented or complex, involving multiple parties, without apparent legitimate justification.
- Copy documents are used in situations where original documentation would be expected, without reasonable explanation.
- There are significant discrepancies in documentation, for example between the description of goods in key documents (i.e. invoices and transport documents) and actual goods shipped, to the extent that this is known.
- The type, quantity and value of goods is inconsistent with the bank's knowledge of the buyer's business.
- The goods transacted are higher risk for money-laundering purposes, for example certain commodities the prices of which can fluctuate significantly, which can make bogus prices difficult to detect.
- The goods transacted require export licences.
- The trade documentation does not comply with applicable laws or standards.
- Unit pricing appears unusual, based on what the bank knows about the goods and trade.
- The transaction is otherwise unusual, for example LCs are frequently amended without a clear rationale or goods are shipped through another jurisdiction for no apparent commercial reason.

162. The following factors may contribute to reducing risk:

- Independent inspection agents have verified the quality and quantity of the goods.

- Transactions involve established counterparties that have a proven track record of transacting with each other and due diligence has previously been carried out.

Customer risk factors

163. The following factors may contribute to increasing risk:

- The transaction and/or the parties involved are out of line with what the bank knows about the customer's previous activity or line of business (e.g. the goods being shipped, or the shipping volumes, are inconsistent with what is known about the importer or exporter's business).

- There are indications that the buyer and seller may be colluding, for example:

  i. the buyer and seller are controlled by the same person;

  ii. transacting businesses have the same address, provide only a registered agent's address, or have other address inconsistencies;

  iii. the buyer is willing or keen to accept or waive discrepancies in the documentation.

- The customer is unable or reluctant to provide relevant documentation to support the transaction.

- The buyer uses agents or third parties.

164. The following factors may contribute to reducing risk:

- The customer is an existing customer whose business is well known to the bank and the transaction is in line with that business.

- The customer is listed on a stock exchange with disclosure requirements similar to the EU's.

Country or geographical risk factors

165. The following factors may contribute to increasing risk:

- A country associated with the transaction (including that where the goods originated from, which they are destined for, or which they transited through, or that where either party to the transaction is based) has currency exchange controls in place. This increases the risk that the transaction's true purpose is to export currency in contravention of local law.

- A country associated with the transaction has higher levels of predicate offences (e.g. those related to the narcotics trade, smuggling or counterfeiting) or free trade zones.

166. The following factors may contribute to reducing risk:

- The trade is within the EU/EEA.
- Countries associated with the transaction have an AML/CFT regime not less robust than that required under Directive (EU) 2015/849 and are associated with low levels of predicate offences.

Measures

167. Banks must carry out CDD on the instructing party. In practice, most banks will only accept instructions from existing customers and the wider business relationship that the bank has with the customer may assist its due diligence efforts.

168. Where a bank provides trade finance services to a customer, it should take steps, as part of its CDD process, to understand its customer's business. Examples of the type of information the bank could obtain include the countries with which the customer trades, which trading routes are used, which goods are traded, who the customer does business with (buyers, suppliers, etc.), whether the customer uses agents or third parties, and, if so, where these are based. This should help banks understand who the customer is and aid the detection of unusual or suspicious transactions.

169. Where a bank is a correspondent, it must apply CDD measures to the respondent. Correspondent banks should follow the guidelines on correspondent banking in Title III, Chapter 1.

Enhanced customer due diligence

170. In higher risk situations, banks must apply EDD. As part of this, banks should consider whether performing more thorough due diligence checks on the transaction itself and on other parties to the transaction (including non-customers) would be appropriate.

171. Checks on other parties to the transaction may include:

- Taking steps to better understand the ownership or background of other parties to the transaction, in particular where they are based in a jurisdiction associated with higher ML/TF risk or where they handle high-risk goods. This may include checks of company registries and third party intelligence sources, and open source internet searches.
- Obtaining more information on the financial situation of the parties involved.

172. Checks on transactions may include:

- using third party or open source data sources, for example the International Maritime Bureau (for warning notices, bills of lading, shipping and pricing checks) or shipping lines' free container tracking service to verify the information provided and to check that the purpose of the transaction is legitimate;

- using professional judgement to consider whether the pricing of goods makes commercial sense, in particular in relation to traded commodities for which reliable and up-to-date pricing information can be obtained;

- checking that the weights and volumes of goods being shipped are consistent with the shipping method.

173. Since LCs and BCs are largely paper-based and accompanied by trade-related documents (e.g. invoices, bills of lading and manifests), automated transaction monitoring may not be feasible. The processing bank should assess these documents for consistency with the terms of the trade transaction and require staff to use professional expertise and judgement to consider whether any unusual features warrant the application of EDD measures or give rise to suspicion of ML/TF.[34]

Simplified customer due diligence

174. The checks banks routinely carry out to detect fraud and ensure the transaction conforms to the standards set by the International Chamber of Commerce mean that, in practice, they will not apply SDD measures even in lower risk situations.

[34] Banks routinely check documents to detect attempts to defraud the bank or its customer. They are a key part of the service provided by a bank offering trade finance. It may be possible for banks to build on these existing controls to meet their AML/CFT obligations.

Chapter 7: Sectoral guidelines for life insurance undertakings

175. Life insurance products are designed to financially protect the policy holder against the risk of an uncertain future event, such as death, illness or outliving savings in retirement (longevity risk). The protection is achieved by an insurer who pools the financial risks that many different policy holders are faced with. Life insurance products can also be bought as investment products or for pension purposes.

176. Life insurance products are provided through different distribution channels to customers who may be natural or legal persons or legal arrangements. The beneficiary of the contract may be the policy holder or a nominated or designated third party; the beneficiary may also change during the term and the original beneficiary may never benefit.

177. Most life insurance products are designed for the long term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds of crime.

178. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapters 5 and 9, may also be relevant in this context. Where intermediaries are used, the delivery channel risk factors set out in Title II, paragraphs 32-33, will be relevant.

179. Intermediaries may also find these guidelines useful.

Risk factors

Product, service and transaction risk factors

180. The following factors may contribute to increasing risk:

- Flexibility of payments, for example the product allows:
  i. payments from unidentified third parties;
  ii. high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments;
  iii. cash payments.
- Ease of access to accumulated funds, for example the product allows partial withdrawals or early surrender at any time, with limited charges or fees.
- Negotiability, for example the product can be:
  i. traded on a secondary market;

ii. used as collateral for a loan.

- Anonymity, for example the product facilitates or allows the anonymity of the customer.

181. Factors that may contribute to reducing risk include:

The product:

- only pays out against a pre-defined event, for example death, or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;
- has no surrender value;
- has no investment element;
- has no third party payment facility;
- requires that total investment is curtailed at a low value;
- is a life insurance policy where the premium is low;
- only allows small-value regular premium payments, for example no overpayment;
- is accessible only through employers, for example a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
- cannot be redeemed in the short or medium term, as in the case of pension schemes without an early surrender option;
- cannot be used as collateral;
- does not allow cash payments;
- has conditions that must be met to benefit from tax relief.

Customer and beneficiary risk factors

182. The following factors may contribute to increasing risk:

- The nature of the customer, for example:

i. legal persons whose structure makes it difficult to identify the beneficial owner;

ii. the customer or the beneficial owner of the customer is a PEP;

iii. the beneficiary of the policy or the beneficial owner of this beneficiary is a PEP;

iv. the customer's age is unusual for the type of product sought (e.g. the customer is very young or very old);

v. the contract does not match the customer's wealth situation;

vi. the customer's profession or activities are regarded as particularly likely to be related to money laundering, for example because they are known to be very cash intensive or exposed to a high risk of corruption;

vii. the contract is subscribed by a 'gatekeeper', such as a fiduciary company, acting on behalf of the customer;

viii. the policy holder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form.

- The customer's behaviour:

i. In relation to the contract, for example:

a. the customer frequently transfers the contract to another insurer;

b. frequent and unexplained surrenders, especially when the refund is done to different bank accounts;

c. the customer makes frequent or unexpected use of 'free look' provisions/'cooling-off' periods, in particular where the refund is made to an apparently unrelated third party;[35]

d. the customer incurs a high cost by seeking early termination of a product;

e. the customer transfers the contract to an apparently unrelated third party;

f. the customer's request to change or increase the sum insured and/or the premium payment are unusual or excessive.

ii. In relation to the beneficiary, for example:

a. the insurer is made aware of a change in beneficiary only when the claim is made;

b. the customer changes the beneficiary clause and nominates an apparently unrelated third party;

[35] A 'free look' provision is a contractual provision, often mandatory under local law, which allows a policy owner or annuitant of a life insurance or annuity contract to examine a contract for a certain number of days and return it for a full refund.

c. the insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are in different jurisdictions.

iii. In relation to payments, for example:

a. the customer uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity;

b. payments from different bank accounts without explanation;

c. payments from banks that are not established in the customer's country of residence;

d. the customer makes frequent or high-value overpayments where this was not expected;

e. payments received from unrelated third parties;

f. catch-up contribution to a retirement plan close to retirement date.

183. The following factors may contribute to reducing risk:

In the case of corporate-owned life insurance, the customer is:

- a credit or financial institution that is subject to requirements to combat money laundering and the financing of terrorism and supervised for compliance with these requirements in a manner that is consistent with Directive (EU) 2015/849;

- a public company listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) that impose requirements to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company;

- a public administration or a public enterprise from an EEA jurisdiction.

Distribution channel risk factors

184. The following factors may contribute to increasing risk:

- non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification documents that comply with Regulation (EU) No 910/2014;

- long chains of intermediaries;

- an intermediary is used in unusual circumstances (e.g. unexplained geographical distance).

185. The following factors may contribute to reducing risk:

- Intermediaries are well known to the insurer, who is satisfied that the intermediary applies CDD measures commensurate to the risk associated with the relationship and in line with those required under Directive (EU) 2015/849.

- The product is only available to employees of certain companies that have a contract with the insurer to provide life insurance for their employees, for example as part of a benefits package.

Country or geographical risk factors

186. The following factors may contribute to increasing risk:

- The insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

- Premiums are paid through accounts held with financial institutions established in jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

- The intermediary is based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

187. The following factors may contribute to reducing risk:

- Countries are identified by credible sources, such as mutual evaluations or detailed assessment reports, as having effective AML/CFT systems.

- Countries are identified by credible sources as having a low level of corruption and other criminal activity.

Measures

188. Article 13(5) of Directive (EU) 2015/849 provides that, for life insurance business, firms must apply CDD measures not only to the customer and beneficial owner but also to the beneficiaries as soon as they are identified or designated. This means that firms must:

- obtain the name of the beneficiary where either a natural or legal person or an arrangement is identified as the beneficiary; or

- obtain sufficient information to be satisfied that the identities of the beneficiaries can be established at the time of payout where the beneficiaries are a class of persons or designated by certain characteristics. For example, where the beneficiary is 'my future grandchildren', the insurer could obtain information about the policy holder's children.

189. Firms must verify the beneficiaries' identities at the latest at the time of payout.

190. Where the firm knows that the life insurance has been assigned to a third party who will receive the value of the policy, they must identify the beneficial owner at the time of the assignment.

Enhanced customer due diligence

191. The following EDD measures may be appropriate in a high-risk situation:

- Where the customer makes use of the 'free look'/'cooling-off' period, the premium should be refunded to the customer's bank account from which the funds were paid. Firms should ensure that they have verified the customer's identity in line with Article 13 of Directive (EU) 2015/849 before making a refund, in particular where the premium is large or the circumstances appear otherwise unusual. Firms should also consider whether the cancellation gives rise to suspicion about the transaction and whether submitting a suspicious activity report would be appropriate.

- Additional steps may be taken to strengthen the firm's knowledge about the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner, the third party payers and payees. Examples include:

  i. not using the derogation in Article 14(2) of Directive (EU) 2015/849, which provides for an exemption from upfront CDD;

  ii. verifying the identity of other relevant parties, including third party payers and payees, before the beginning of the business relationship;

  iii. obtaining additional information to establish the intended nature of the business relationship;

  iv. obtaining additional information on the customer and updating more regularly the identification data of the customer and beneficial owner;

  v. if the payer is different from the customer, establishing the reason why;

  vi. verifying identities on the basis of more than one reliable and independent source;

  vii. establishing the customer's source of wealth and source of funds, for example employment and salary details, inheritance or divorce settlements;

  viii. where possible, identifying the beneficiary at the beginning of the business relationship, rather than waiting until they are identified or designated, bearing in mind that the beneficiary can change over the term of the policy;

  ix. identifying and verifying the identity of the beneficiary's beneficial owner;

x. in line with Articles 20 and 21 of Directive (EU) 2015/849, taking measures to determine whether the customer is a PEP and taking reasonable measures to determine whether the beneficiary or the beneficiary's beneficial owner is a PEP at the time of assignment, in whole or in part, of the policy or, at the latest, at the time of payout;

xi. requiring the first payment to be carried out through an account in the customer's name with a bank subject to CDD standards that are not less robust than those required under Directive (EU) 2015/849.

192. Article 20 of Directive (EU) 2015/849 requires that, where the risk associated with a PEP relationship is high, firms must not only apply CDD measures in line with Article 13 of the Directive but also inform senior management before the payout of the policy so that senior management can take an informed view of the ML/TF risk associated with the situation and decide on the most appropriate measures to mitigate that risk; in addition, firms must conduct EDD on the entire business relationship.

193. More frequent and more in-depth monitoring of transactions may be required (including where necessary, establishing the source of funds).

Simplified customer due diligence

194. The following measures may satisfy some of the CDD requirements in low-risk situations (to the extent permitted by national legislation):

- Firms may be able to assume that the verification of the identity of the customer is fulfilled on the basis of a payment drawn on an account that the firm is satisfied is in the sole or joint name of the customer with an EEA-regulated credit institution.

- Firms may be able to assume that the verification of the identity of the beneficiary of the contract is fulfilled on the basis of a payment made to an account in the beneficiary's name at a regulated EEA credit institution.

Chapter 8: Sectoral guidelines for investment firms

195. Investment management is the management of an investor's assets to achieve specific investment goals. It includes both discretionary investment management, where investment managers take investment decisions on their customers' behalf, and advisory investment management, where investment managers advise their customers on which investments to make but do not execute transactions on their customers' behalf.

196. Investment managers usually have a limited number of private or institutional customers many of which are wealthy, for example high-net-worth individuals, trusts, companies, government agencies and other investment vehicles. The customers' funds are often handled by a local custodian, rather than the investment manager. The ML/TF risk associated with investment management is therefore driven primarily by the risk associated with the type of customers investment managers serve.

197. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapter 5, may also be relevant in this context.

Risk factors

Product, service or transaction risk factors

198. The following factors may contribute to increasing risk:

- transactions are unusually large;
- third party payments are possible;
- the product or service is used for subscriptions that are quickly followed by redemption possibilities, with limited intervention by the investment manager.

Customer risk factors

199. The following factors may contribute to increasing risk:

- The customer's behaviour, for example:
  i. the rationale for the investment lacks an obvious economic purpose;
  ii. the customer asks to repurchase or redeem a long-term investment within a short period after the initial investment or before the payout date without a clear rationale, in particular where this results in financial loss or payment of high transaction fees;
  iii. the customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale;

iv. unwillingness to provide CDD information on the customer and the beneficial owner;

v. frequent changes to CDD information or payment details;

vi. the customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed;

vii. the circumstances in which the customer makes use of the 'cooling-off' period give rise to suspicion;

viii. using multiple accounts without previous notification, especially when these accounts are held in multiple or high-risk jurisdictions;

ix. the customer wishes to structure the relationship in such a way that multiple parties, for example nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

- The customer's nature, for example:

i. the customer is a company or trust established in a jurisdiction associated with higher ML/TF risk (firms should pay particular attention to those jurisdictions that do not comply effectively with international tax transparency standards);

ii. the customer is an investment vehicle that carries out little or no due diligence on its own clients;

iii. the customer is an unregulated third party investment vehicle;

iv. the customer's ownership and control structure is opaque;

v. the customer or the beneficial owner is a PEP or holds another prominent position that might enable them to abuse their position for private gain;

vi. the customer is a non-regulated nominee company with unknown shareholders.

- The customer's business, for example the customer's funds are derived from business in sectors that are associated with a high risk of financial crime.

200. The following factors may contribute to reducing risk:

- The customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme.

- The customer is a government body from an EEA jurisdiction.

- The customer is a financial institution established in an EEA jurisdiction.

Country or geographical risk factors

201. The following factors may contribute to increasing risk:

- The investor or their custodian is based in a jurisdiction associated with higher ML/TF risk.
- The funds come from a jurisdiction associated with higher ML/TF risk.

Measures

202. Investment managers typically need to develop a good understanding of their customers to help them identify suitable investment portfolios. The information gathered will be similar to that which firms obtain for AML/CFT purposes.

203. Firms should follow the EDD guidelines set out in Title II in higher risk situations. In addition, where the risk associated with a business relationship is high, firms should:

- identify and, where necessary, verify the identity of the underlying investors of the firm's customer where the customer is an unregulated third party investment vehicle;
- understand the reason for any payment or transfer to or from an unverified third party.

204. To the extent permitted by national legislation, investment managers may apply the SDD guidelines set out in Title II in low-risk situations.

Chapter 9: Sectoral guidelines for providers of investment funds

205. The provision of investment funds can involve multiple parties: the fund manager, appointed advisers, the depositary and sub-custodians, registrars and, in some cases, prime brokers. Similarly, the distribution of these funds can involve parties such as tied agents, advisory and discretionary wealth managers, platform service providers and independent financial advisers.

206. The type and number of parties involved in the funds distribution process depends on the nature of the fund and may affect how much the fund knows about its customer and investors. The fund or, where the fund is not itself an obliged entity, the fund manager will retain responsibility for compliance with AML/CFT obligations, although aspects of the fund's CDD obligations may be carried out by one or more of these other parties subject to certain conditions.

207. Investment funds may be used by persons or entities for ML/TF purposes:

- Retail funds are often distributed on a non-face-to-face basis; access to such funds is often easy and relatively quick to achieve, and holdings in such funds can be transferred between different parties.

- Alternative investment funds, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). Funds that are designed for a limited number of high-net-worth individuals, or for family offices, can have an inherently higher risk of abuse for ML/TF purposes than retail funds, since investors are more likely to be in a position to exercise control over the fund assets. If investors exercise control over the assets, such funds are personal asset-holding vehicles, which are mentioned as a factor indicating potentially higher risk in Annex III to Directive (EU) 2015/849.

- Notwithstanding the often medium- to long-term nature of the investment, which can contribute to limiting the attractiveness of these products for money laundering purposes, they may still appeal to money launderers on the basis of their ability to generate growth and income.

208. This chapter is directed at:

a) investment fund managers performing activities under Article 3(2)(a) of Directive (EU) 2015/849; and

b) investment funds marketing their own shares or units, under Article 3(2)(d) of Directive (EU) 2015/849.

Other parties involved in the provision or distribution of the fund, for example intermediaries, may have to comply with their own CDD obligations and should refer to relevant chapters in these guidelines as appropriate.

209. For funds and fund managers, the sectoral guidelines in Title III, Chapters 1, 7 and 8, may also be relevant.

Risk factors

Product, service or transaction risk factors

210. The following factors may contribute to increasing the risk associated with the fund:

- The fund is designed for a limited number of individuals or family offices, for example a private fund or single investor fund.
- It is possible to subscribe to the fund and then quickly redeem the investment without the investor incurring significant administrative costs.
- Units of or shares in the fund can be traded without the fund or fund manager being notified at the time of the trade and, as a result, information about the investor is divided among several subjects (as is the case with closed-ended funds traded on secondary markets).

211. The following factors may contribute to increasing the risk associated with the subscription:

- The subscription involves accounts or third parties in multiple jurisdictions, in particular where these jurisdictions are associated with a high ML/TF risk as defined in paragraphs 22-27 of Title II of the guidelines.
- The subscription involves third party subscribers or payees, in particular where this is unexpected.

212. The following factors may contribute to reducing the risk associated with the fund:

- Third party payments are not allowed.
- The fund is open to small-scale investors only, with investments capped.

Customer risk factors

213. The following factors may contribute to increasing risk:

- The customer's behaviour is unusual, for example:

  i. The rationale for the investment lacks an obvious strategy or economic purpose or the customer makes investments that are inconsistent with the customer's overall financial situation, where this is known to the fund or fund manager.

  ii. The customer asks to repurchase or redeem an investment within a short period after the initial investment or before the payout date without a clear rationale,

in particular where this results in financial loss or payment of high transaction fees.

iii. The customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale.

iv. The customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed.

v. The customer uses multiple accounts without previous notification, especially when these accounts are held in multiple jurisdictions or jurisdictions associated with higher ML/TF risk.

vi. The customer wishes to structure the relationship in such a way that multiple parties, for example non-regulated nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

vii. The customer suddenly changes the settlement location without rationale, for example by changing the customer's country of residence.

viii. The customer and the beneficial owner are located in different jurisdictions and at least one of these jurisdictions is associated with higher ML/TF risk as defined in the general part of the guidelines.

ix. The beneficial owner's funds have been generated in a jurisdiction associated with higher ML/TF risk, in particular where the jurisdiction is associated with higher levels of predicate offences to ML/TF.

214. The following factors may contribute to reducing risk:

- the customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme;
- the customer is a firm in an EEA country or a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Distribution channel risk factors

215. The following factors may contribute to increasing risk:

- unclear or complex distribution channels that limit the fund's oversight of its business relationships and restrict its ability to monitor transactions, for example the fund uses a large number of sub-distributors for distribution in third countries;
- the distributor is located in a jurisdiction associated with higher ML/TF risk as defined in the general part of these guidelines.

216. The following factors may indicate lower risk:

- The fund admits only a designated type of low-risk investor, such as regulated firms investing as a principal (e.g. life companies) or corporate pension schemes.

- The fund can be purchased and redeemed only through a firm, for example a financial intermediary, in an EEA country or a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Country or geographical risk factors

217. The following factors may contribute to increasing risk:

- Investors' monies have been generated in jurisdictions associated with higher ML/TF risk, in particular those associated with higher levels of predicate offences to money laundering.

- The fund or fund manager invests in sectors with higher corruption risk (e.g. the extractive industries or the arms trade) in jurisdictions identified by credible sources as having significant levels of corruption or other predicate offences to ML/TF, in particular where the fund is a single investor fund or has a limited number of investors.

Measures

218. The measures funds or fund managers should take to comply with their CDD obligations will depend on how the customer or the investor (where the investor is not the customer) comes to the fund. The fund or fund manager should also take risk-sensitive measures to identify and verify the identity of the natural persons, if any, who ultimately own or control the customer (or on whose behalf the transaction is being conducted), for example by asking the prospective investor to declare, when they first apply to join the fund, whether they are investing on their own behalf or whether they are an intermediary investing on someone else's behalf.

219. The customer is:

a) a natural or legal person who directly purchases units of or shares in a fund on their own account, and not on behalf of other, underlying investors; or

b) a firm that, as part of its economic activity, directly purchases units of or shares in its own name and exercises control over the investment for the ultimate benefit of one or more third parties who do not control the investment or investment decisions; or

c) a firm, for example a financial intermediary, that acts in its own name and is the registered owner of the shares or units but acts on the account of, and pursuant to specific instructions from, one or more third parties (e.g. because the financial intermediary is a nominee, broker, multi-client pooled account/omnibus type account operator or operator of a similar passive-type arrangement); or

d) a firm's customer, for example a financial intermediary's customer, where the firm is not the registered owner of the shares or units (e.g. because the investment fund uses a financial intermediary to distribute fund shares or units, and the investor purchases units or shares through the firm and the firm does not become the legal owner of the units or shares).

SDD and EDD measures to be taken in the situations described in paragraphs 219a and 219b

220. In the situations described in paragraphs 219a and 219b, examples of EDD measures a fund or fund manager should apply in high-risk situations include:

- obtaining additional customer information, such as the customer's reputation and background, before the establishment of the business relationship;
- taking additional steps to further verify the documents, data or information obtained;
- obtaining information on the source of funds and/or the source wealth of the customer and of the customer's beneficial owner;
- requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer;
- increasing the frequency and intensity of transaction monitoring;
- requiring that the first payment is made through a payment account held in the sole or joint name of the customer with an EEA-regulated credit or financial institution or a regulated credit or financial institution in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849;
- obtaining approval from senior management at the time of the transaction when a customer uses a product or service for the first time;
- enhanced monitoring of the customer relationship and individual transactions.

221. In lower risk situations, to the extent permitted by national legislation, and provided that the funds are verifiably being transferred to or from a payment account held in the customer's sole or joint name with an EEA-regulated credit or financial institution, an example of the SDD measures the fund or fund manager may apply is using the source of funds to meet some of the CDD requirements.

SDD and EDD measures to be taken in situations described in paragraph 219c

222. In the situations described in paragraph 219c, where the financial intermediary is the fund or fund manager's customer, the fund or fund manager should apply risk-sensitive CDD measures to the financial intermediary. The fund or fund manager should also take risk-sensitive measures to identify, and verify the identity of, the investors underlying the financial intermediary, as these investors are beneficial owners of the funds invested through the intermediary. To the extent permitted by national law, in low-risk situations, funds or fund managers may apply SDD measures similar to those described in

paragraph 112 of these guidelines, subject to the following conditions:

- The financial intermediary is subject to AML/CFT obligations in an EEA jurisdiction or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

- The financial intermediary is effectively supervised for compliance with these requirements.

- The fund or fund manager has taken risk-sensitive steps to be satisfied that the ML/TF risk associated with the business relationship is low, based on, inter alia, the fund or fund manager's assessment of the financial intermediary's business, the types of clients the intermediary's business serves and the jurisdictions the intermediary's business is exposed to.

- The fund or fund manager has taken risk-sensitive steps to be satisfied that the intermediary applies robust and risk-sensitive CDD measures to its own customers and its customers' beneficial owners. As part of this, the fund or fund manager should take risk-sensitive measures to assess the adequacy of the intermediary's CDD policies and procedures, for example by referring to publicly available information about the intermediary's compliance record or liaising directly with the intermediary.

- The fund or fund manager has taken risk-sensitive steps to be satisfied that the intermediary will provide CDD information and documents on the underlying investors immediately upon request, for example by including relevant provisions in a contract with the intermediary or by sample-testing the intermediary's ability to provide CDD information upon request.

223. Where the risk is increased, in particular where the fund is designated for a limited number of investors, EDD measures must apply and may include those set out in paragraph 220 above.

SDD and EDD measures to be taken in situations described in paragraph 219d

224. In the situations described in paragraph 219d, the fund or fund manager should apply risk-sensitive CDD measures to the ultimate investor as the fund or fund manager's customer. To meet its CDD obligations, the fund or fund manager may rely upon the intermediary in line with, and subject to, the conditions set out in Chapter II, Section 4, of Directive (EU) 2015/849.

225. To the extent permitted by national law, in low-risk situations, funds or fund managers may apply SDD measures. Provided that the conditions listed in paragraph 222 are met, SDD measures may consist of the fund or fund manager obtaining identification data from the fund's share register, together with the information specified in Article 27(1) of Directive (EU) 2015/849, which the fund or fund manager must obtain from the intermediary within a reasonable timeframe. The fund or fund manager should set that timeframe in line with the risk-based approach.

226. Where the risk is increased, in particular where the fund is designated for a limited number of investors, EDD measures must apply and may include those set out in

paragraph 220 above.

Title IV – Implementation

Implementation

227. Competent authorities and firms should comply with these guidelines by 26 June 2018.

4. Accompanying documents

4.1. Impact assessment

Introduction

1. Directive (EU) 2015/849 places the risk-based approach at the centre of the Union's AML/CFT regime. It makes clear that the risk of ML/TF can vary and states that a risk-based approach helps effectively to manage that risk. What credit and financial institutions ('firms') do to understand who their customers are is central to this process.

2. Directive (EU) 2015/849 requires the ESAs to issue guidelines to competent authorities and firms on the risk factors firms should take into consideration and the measures they should take in situations where simplified or enhanced CDD would be appropriate. The aim is to promote a common understanding, by firms and competent authorities, of what the risk-based approach to AML/CFT entails and how it should be applied.

Scope and objectives

3. This impact assessment describes the policy options the ESAs considered when drafting these guidelines and sets out how these options might affect their stakeholders.

4. The ESAs considered the views of AML/CFT competent authorities, existing cost-benefit analyses and the Commission Staff's impact assessment of its proposal for a fourth Anti-Money Laundering Directive. They found that the application of these guidelines would not give rise to significant costs over and above those that firms and competent authorities would incur as a result of the underlying legal obligations set out in Directive (EU) 2015/849.

5. The ESAs therefore considered that it would not be proportionate to carry out a full, quantitative assessment of the costs and benefits arising from the application of the proposed guidelines by competent authorities and firms. Instead, this impact assessment examines, in qualitative terms, the impact that these guidelines would have if all firms and competent authorities fully complied with them. This means that the estimated net impact of the preferred options should be interpreted as the maximum impact of the full implementation of the proposed guidelines; the impact of the actual implementation of these guidelines could be less.

Baseline

6. Article 17 of Directive (EU) 2015/849 requires the ESAs to issue guidelines on the risk factors to be taken into consideration and the measures to be taken in situations where SDD measures are appropriate.

7. Article 18(4) of Directive (EU) 2015/849 requires the ESAs to issue guidelines on the risk factors to be taken into consideration and the measures to be taken in situations where

EDD measures are appropriate.

8. In both cases, the ESAs have to take specific account of the nature and size of firms' business.

9. The ESAs considered options in relation to

- the consistency of these guidelines with international AML/CFT standards;
- the structure of these guidelines;
- the guidelines' addressees; and
- the level of prescription.

Consistency with international AML/CFT standards

10. The ESAs have not issued guidelines on ML/TF risk factors or simplified and enhanced CDD so far. However, relevant guidance has been published by international standard setters, including the FATF and the Basel Committee on Banking Supervision.

Option 1

11. The ESAs' guidelines could reproduce, or simply refer to, international standards and guidance on ML/TF risk factors and simplified and enhanced CDD.

12. The advantage of this approach is that it consolidates existing guidance and makes compliance easier for firms with an international footprint.

13. The disadvantage is that existing international guidance is insufficient, by itself, to meet the requirements of Articles 17 and 18(4) of Directive (EU) 2015/849. This is because international guidance does not:

- take into account specific measures set out in Directive (EU) 2015/849, for example in relation to certain electronic money products or high-risk third countries that have been identified by the Commission as posing significant risks to the Union's financial system;
- cover all the financial sectors included in Directive (EU) 2015/849's scope; or
- contain sufficient detail to ensure the consistent application of Directive (EU) 2015/849's risk-based approach.

Option 2

14. The ESAs' guidelines could be drafted in a way that is consistent with existing international standards and guidance.

15. The advantage of this approach is that it allows the ESAs to address provisions that are

specific to Directive (EU) 2015/849 and tailor their approach to those financial sectors within Directive (EU) 2015/849's scope. It also allows the drafting of the guidelines in a way that is conducive to the consistent and coherent application of the risk-based approach by firms and competent authorities across the EU.

16. The disadvantage is that there is a risk that amendments to, or new, international guidelines may not be consistent with the ESAs' guidelines. This approach would therefore mean reviewing and, where necessary, updating the guidelines periodically and whenever international standard setters reconsider their guidance and standards.

Option 3

17. The ESAs' guidelines could be drafted without regard to international standards and guidance.

18. The advantage of this approach is that it allows the ESAs to issue guidelines specific to the European context.

19. The disadvantage of this approach is that it risks exposing Member States to international censure should their approach be in breach of international standards.

Preferred option

20. Option 2 is the ESAs' preferred option because it allows firms and competent authorities to comply with international standards and guidelines while fostering the consistent and coherent application of the risk-based approach across the EU.

Structure of the guidelines

21. The ESAs have two mandates to issue guidelines on risk factors and CDD, one in relation to high-risk situations and one in relation to low-risk situations.

Option 1

22. The ESAs could issue two sets of guidelines.

23. The advantage of this approach is that this might result in two sets of short guidelines.

24. The disadvantage is that separate guidelines risk being duplicative, as it is not enough, under a risk-based approach, to consider either high-risk or low-risk factors only: firms should always consider all relevant risk factors in order to obtain a holistic view of the risk to which they are exposed and manage that risk appropriately.

Option 2

25. The ESAs could issue a single set of guidelines on both simplified and enhanced CDD.

26. The advantage of this approach is that a single set of guidelines is more conducive to

firms and competent authorities obtaining a holistic view of the risk associated with individual business relationships and occasional transactions than are separate guidelines on high and low risk.

27. The disadvantage is that these more complex guidelines may be more difficult to navigate for firms with less previous exposure to AML/CFT issues and the risk-based approach.

Preferred option

28. Option 2 is the ESAs' preferred approach as it better reflects how firms and competent authorities should implement the risk-based approach.

Addressees

29. Directive (EU) 2015/849 requires that the ESAs take account of the nature and size of firms' business.

Option 1

30. The ESAs could issue one set of guidelines for all firms.

31. The advantage of this approach is that it ensures the development of a consistent approach to the application of the risk-based approach across the entire financial services industry.

32. The disadvantage is that this approach does not take into account the diversity of Europe's financial sector and risks being unduly prescriptive, ineffective or onerous for at least some firms.

Option 2

33. The ESAs could draft guidelines for each sector.

34. The advantage of this approach is that it allows the development of guidelines in a targeted, proportionate and effective way, which takes into account the nature and size of different types of firms.

35. The disadvantage is that it does not lend itself to the development of a consistent European approach to AML/CFT.

Option 3

36. The ESAs could draft guidelines that apply to all firms and supplement these with sector-specific guidelines.

37. The advantage of this option is that it facilitates both the development of a common understanding of the risk-based approach and the drafting of targeted guidelines that take account of the specificities of firms in key sectors. This should be conducive to more consistent practices and supervisory expectations.

38. The disadvantage is that there is a risk that some firms will only have regard to the sector-specific guidelines, which are incomplete on their own. This would mean that these firms' AML/CFT systems and controls would be unlikely to be effective.

Preferred option

39. Option 3 is the ESAs' preferred option, as it benefits from the advantages associated with Options 1 and 2 while effectively mitigating their disadvantages.

Level of prescription

40. Directive (EU) 2015/849 identifies a number of situations that firms must always treat as high risk. In some cases, Directive (EU) 2015/849 prescribes what firms must do to mitigate that risk. However, most of Directive (EU) 2015/849 contains only high-level principles and obligations.

Option 1

41. The guidelines could set out exactly what constitutes high and low risk and what firms should do in each of these situations.

42. The advantage of this approach is that a high level of prescription could reduce regulatory uncertainty and harmonise approaches across the EU. In some cases, it could also reduce the cost of compliance, as firms would not have to risk-assess individual business relationships or occasional transactions.

43. The disadvantage is that this approach is unlikely to be proportionate or effective, as firms and competent authorities will focus on compliance rather than the successful identification, assessment and management of ML/TF risk.

44. This approach also fails to take account of contextual factors that could move a business relationship or occasional transaction into a higher or lower risk category. For example, setting monetary thresholds below which a relationship should be considered low risk at European level may lead to the application of inadequate risk mitigation measures in jurisdictions where this threshold does not reflect average incomes. There is also a risk that prescribing high- and low-risk situations will lead to firms failing to identify and manage high-risk situations that are not set out in the guidelines.

45. Finally, this approach is not compatible with international AML/CFT standards and guidance.

Option 2

46. The guidelines could provide firms with information on what they need to consider when determining whether a situation presents a high or a low ML/TF risk, and which type of CDD might be appropriate to manage that risk.

47. The advantage of this approach is that it allows firms to develop a good understanding of the ML/TF risk to which they are exposed. It also enables them to focus their resources on areas of high risk, which is conducive to the adoption of proportionate and effective

AML/CFT controls.

48. The disadvantage of this approach is that it requires firms and competent authorities to have sufficient AML/CFT expertise to identify, assess and manage ML/TF risk effectively.

Preferred option

49. Option 2 is the ESAs' preferred approach, as it is conducive to the adoption, by firms, of a proportionate and effective risk-based approach.

Costs and benefits

50. The ESAs' preferred options are guidelines that:

- are consistent with relevant international standards and guidance;
- address both high and low risk factors;
- combine general guidelines for all firms with sector-specific guidelines; and
- provide firms with the tools they need to identify, assess and manage ML/TF risk in a proportionate and effective manner.

51. The ESAs expect firms and competent authorities to incur at times significant costs as they review and make changes to their approaches to comply with new national legal frameworks resulting from the transposition of Directive (EU) 2015/849 by Member States. The cost associated with the application of these guidelines will therefore be largely absorbed by the cost associated with compliance with the underlying legal change.

52. This means that these guidelines should not create significant costs for firms or competent authorities above those associated with a move to the new legal AML/CFT regime under Directive (EU) 2015/849. The benefits will follow largely from risk-sensitive guidelines, clear regulatory expectations and the harmonisation of approaches across the EU.

Firms

53. The benefits of this approach for firms are that these guidelines allow firms to adopt policies and procedures that are proportionate to the nature, scale and complexity of their activities. This means that more complex, higher risk, firms will be able to tailor their risk management to their risk profile, and firms that are exposed to low levels of ML/TF risk will be able to adjust their compliance costs accordingly.

54. All firms will face some one-off costs as a result of reviewing their internal policies and controls, making necessary adjustments to reflect these guidelines and training staff accordingly. These one-off costs will be higher for more complex firms and firms that do not already apply a risk-based approach.

55. However, these one-off costs are likely to be offset by all firms in the medium to long

term through ongoing cost reductions once the necessary adjustments have been made; furthermore, since these adjustments are likely to take place at the same time as new legislation transposing Directive (EU) 2015/849 come into effect, firms should be able to absorb the one-off costs associated with these guidelines as part of the changes they have to make to comply with their new legal and regulatory obligations. This means that the costs attributable to these guidelines will not in the end be significant.

56. In light of the considerations regarding costs and benefits set out above, the net impact of these guidelines for firms is likely to be close to zero.

Competent authorities

57. The benefits of this approach for competent authorities are that the guidelines will help supervisors set clear expectations of the factors firms should consider when identifying and assessing ML/TF risk and deciding on the appropriate level of CDD.

58. The costs to competent authorities will arise mainly from reviewing existing regulatory guidance to firms and supervisory manuals to ensure consistency with these guidelines. Competent authorities will also incur some costs from retraining staff. However, all of these costs are likely to be one-off costs that are likely to be absorbed as part of their normal work by those competent authorities that already enforce a risk-based approach. The one-off costs will be higher for competent authorities that are unfamiliar with the risk-based approach, but they are unlikely to exceed the costs arising from the implementation of national legislation transposing Directive (EU) 2015/849.

59. In light of the considerations regarding costs and benefits set out above, the net impact of these guidelines for competent authorities is expected to be close to zero, but positive.

4.2. Overview of questions for consultation

a) Do you consider that these guidelines are conducive to firms adopting risk-based, proportionate and effective AML/CFT policies and procedures in line with the requirements set out in Directive (EU) 2015/849?

b) Do you consider that these guidelines are conducive to competent authorities effectively monitoring firms' compliance with applicable AML/CFT requirements in relation to individual risk assessments and the application of both simplified and enhanced customer due diligence measures?

c) The guidelines in Title III of this consultation paper are organised by types of business. Respondents to this consultation paper are invited to express their views on whether such an approach gives sufficient clarity on the scope of application of the AMLD to the various entities subject to its requirements or whether it would be preferable to follow a legally-driven classification of the various sectors; for example, for the asset management sector, this would mean referring to entities covered by Directive 2009/65/EC and Directive 2011/61/EU and for the individual portfolio management or investment advice activities, or entities providing other investment services or activities, to entities covered by Directive 2014/65/EU.

4.3. Views of the stakeholder groups

60. The EBA's Banking Stakeholder Group (BSG) responded to this consultation.

61. The BSG considered that the draft guidelines were conducive to firms adopting risk-based AML/CFT policies and procedures. However, in some cases, greater detail was warranted to reduce the risk of national competent authorities enforcing divergent expectations of firms' assessment and management of AML/CFT risk, for example in relation to establishing a beneficial owner's source of funds, the application of CDD measures to non-face-to-face relationships and the appropriate management of lower risk correspondent banking relationships.

62. The BSG also asked for greater clarity on the relationship between these guidelines and similar international or national AML/CFT guidance.

4.4. Feedback on the public consultation

63. The ESAs publicly consulted on the draft proposal.

64. The consultation period lasted for three months and ended on 22 January 2016. Fifty-seven responses were received from representatives of or associations from the private sector, of which forty-five were published on the ESAs' websites. The EBA's Banking Stakeholder Group was among those who expressed a view.

65. This paper summarises the key points and other comments received during the public consultation, the ESAs' response and the action taken to address these comments.

66. Where several respondents made similar comments or the same respondent repeated their comments in response to different questions, these comments, and the ESAs' analysis, are included in the section of this paper where the ESAs considered them most appropriate.

67. Several changes to the draft joint guidelines have been made as a result of the responses received during the public consultation.

Summary of key issues and the ESAs' response

68. Most respondents welcomed the draft guidelines. They considered that the draft guidelines would foster a common understanding of the risk-based approach to AML/CFT and support the implementation, by firms, of an effective and proportionate risk-based approach to AML/CFT at the national level. Respondents were particularly supportive of the draft guidelines' emphasis on firms taking a holistic view of all relevant risk factors when determining the level of risk associated with a business relationship or occasional transaction, and generally found the level of detail the draft guidelines contained to be adequate.

69. Where respondents raised concerns, these broadly fell into four categories:

- the ability or preparedness of national competent authorities to apply these draft guidelines in a consistent manner;
- the status of these draft guidelines, in particular their relationship with existing national and international guidelines;
- the distinction between money laundering and terrorist financing risk factors; and
- a perceived conflict between the draft guidelines' provisions and a customer's right to a basic payment account on the one hand and the Union's data protection framework on the other.

70. The ESAs thank all respondents for taking the time to reply and for the constructive and positive feedback they received. The ESAs have carefully considered all responses and revised the guidelines where appropriate.

Ensuring the consistent application of these guidelines by national competent authorities

71. A number of respondents were concerned that these guidelines, of themselves, might not be enough to ensure the consistent supervision, by national competent authorities, of the risk-based approach to AML/CFT. Several respondents thought that the ESAs should take further action to achieve greater harmonisation of supervisory approaches across Member States and one respondent called on the ESAs to act as arbiters should firms disagree with their competent authorities' assessments.

72. These guidelines form part of the ESAs' wider work on fostering consistent supervisory practices and a common approach to AML/CFT, and need to be considered in that context. The Risk Factors Guidelines equip firms with the tools they need to make informed decisions on the effective identification, assessment and management of ML/TF risk, and set common, regulatory expectations to which national competent authorities will refer when assessing the adequacy of firms' AML/CFT systems and controls. Other ESA instruments, including the Joint Risk-Based Supervision Guidelines,36 complement the Risk Factors Guidelines by specifying how competent authorities should organise AML/CFT supervision. Together, they provide a solid foundation for promoting a coherent and more harmonised supervisory response to AML/CFT challenges.

73. As in other areas of their work, the ESAs are providing training to competent authorities on the application of their AML/CFT standards, monitoring their implementation and keeping them under review to ensure that they remain relevant and conducive to a more robust European approach to AML/CFT. Should the ESAs become aware of competent authorities failing to apply these standards, or applying them in a way that appears to be in breach of Union law, they will take action to address this where appropriate and necessary.

The status of these draft guidelines, in particular their relationship with existing national and international guidelines

74. Several respondents sought clarity on how these guidelines sit alongside national or international AML/CFT standards such as the FATF's Recommendations and the Wolfsberg Group's AML/CFT guidance. Some thought that a number of provisions in these guidelines went beyond what international best practice suggested and called on the ESAs to reconsider their approach; consistency was important to make AML/CFT compliance easier for firms with an international footprint. One respondent wrote that they preferred national industry guidance and would be following that instead.

75. The ESAs drafted these guidelines in a way that is consistent with existing international standards and guidance. This is in line with the co-legislators' approach to Directive (EU) 2015/849, which provides a common European legal basis for the implementation of the FATF's Recommendations.

[36] Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis (2016): https://esas-joint-committee.europa.eu/Pages/Guidelines/Joint-Guidelines-on-the-Characteristics-of-a-Risk-based-Approach-to-Anti-money-Laundering-and-Terrorist-Financing-Supervisi.aspx.

76. There are, however, a number of differences between international guidance and the EU's legal framework, for example in situations where EU law creates specific obligations on firms. Regulatory guidance cannot over-ride legal provisions and, in those cases, these guidelines necessarily differ from international standards.

77. Article 16(3) of the ESAs Regulations requires competent authorities to 'make every effort to comply' with these guidelines. In practice, this means that competent authorities will incorporate these guidelines into their national framework by, for example, amending relevant legal provisions or adjusting supervisory guidance. Firms that do not adapt their approach accordingly risk being in breach of their AML/CFT obligations.

Consistency with legal provisions in Union law

78. Some respondents were concerned that compliance with these guidelines' provisions would result in a breach of a person's right to a basic payment account under Directive 2014/92/EU or the European data protection framework. One respondent in particular was concerned that expecting firms to consider a customer's reputation was against data protection rules.

79. Directive (EU) 2015/849 makes the identification and assessment of ML/TF risk and the successful application of risk-sensitive CDD controls to all customers and their beneficial owners a condition for the establishment of a business relationship. Where firms cannot comply with these obligations, they cannot enter into, or maintain, a business relationship.

80. Consequently,

- Directive 2014/92/EU provides that the right to open and use a basic payment account applies only to the extent that credit institutions can comply with their AML/CFT obligations; and

- Article 43 of Directive (EU) 2015/849 is clear that the processing of personal data for AML/CFT purposes is a matter of public interest under Directive 95/46/EC. This means that firms that collect, analyse, record or otherwise handle personal data to, for example, assess the ML/TF risk associated with a particular customer but do not use that personal data for purposes other than AML/CFT compliance, are not in breach of the Union's data protection framework.

81. These guidelines therefore comply with Union law and do not conflict with provisions in Directive 2014/92/EU or data protection rules.

Distinguishing money laundering and terrorist financing risk factors

82. A number of respondents asked for further guidance on the risks of terrorist financing, and how CFT controls are different from AML controls.

83. These guidelines do not systematically distinguish between the systems and controls firms should put in place to identify, assess and manage ML risk and those they should put in place to identify, assess and manage TF risk; guidance related to one will be relevant for the other, unless specified. This is because terrorist funds can appear legitimate and inoffensive, and, in the absence of specific intelligence from law enforcement, will be difficult to identify. The value in CFT controls therefore lies mainly in the post facto identification of terrorist networks, and, consequently, the CFT systems and controls firms will put in place, such as monitoring and other CDD measures, overlap with their AML systems and controls.

84. Attempts are now being made at the international, supranational and national levels to better understand TF risk and identify risk factors that may be conducive to a more preventative approach. These risk factors will be incorporated into these guidelines as appropriate.

Summary of responses to the consultation and the ESAs' analysis

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
Comments on Title I			
Subject matter, scope and definitions	One respondent was concerned that the definition of 'occasional transaction' was not in line with the definition in Directive (EU) 2015/849.	Transactions can be carried out as part of a business relationship, or on a one-off, 'occasional' basis where a business relationship has not been established. As Directive (EU) 2015/849 makes clear, a business relationship 'is expected, at the time when the contact is established, to have an element of duration'. There is no expectation of an ongoing, durable relationship in the case of occasional transactions and the guidelines' definition of occasional transactions – that is, a transaction that is not carried out as part of a business relationship – is therefore in line with Directive (EU) 2015/849.	No change.
	One respondent wanted to replace 'firms' with 'obliged entities'.	'Obliged entities', for the purpose of Directive (EU) 2015/849, include some entities that are not credit or financial institutions. These guidelines apply to credit and financial institutions only.	No change.
	One respondent asked that the guidelines define 'must', 'may' and 'should'.	In line with other ESA guidelines, the Risk Factors Guidelines use 'must', 'should' and 'may' to describe different degrees of obligations on firms. 'Must' is used to describe a legal obligation, 'should' introduces a strong expectation and 'may' describes examples of possible measures firms could take to meet their legal and regulatory obligations.	Several, to identify the legal source whenever the word 'must' is used.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
Comments on Title II			
Assessing and managing risk – general comments	One respondent thought that firms should not be expected to do their own risk assessment. This was something national authorities should do.	Article 8 of Directive (EU) 2015/849 requires firms to identify and assess the ML/TF risk to which they are exposed.	No change.
	A number of respondents disagreed with individual risk factors, e.g. 'large transactions'. They did not believe they were indicators of higher risk.	The risk factors listed in Title II of these guidelines are not absolute and will not necessarily, of themselves, move a relationship into a higher risk category. The guidelines are clear that the overall context is important and that firms should take a holistic view of all relevant risk factors.	No change.
	One respondent considered that the guidelines' expectation that documents be kept up to date was excessive, and that firms should merely do this on a best-efforts basis	Article 13(1)(d) of Directive (EU) 2015/849 requires firms to keep documents, data or information held up to date.	No change.
	A number of respondents questioned the rationale for requiring firms to establish the nature and purpose of the business relationship, with some suggesting that this was not essential.	Establishing the nature and purpose of the business relationship is not only a requirement under Directive (EU) 2015/849, it is also central to understanding the ML/TF risk associated with the business relationship and will help firms determine what constitutes an unusual or suspicious transaction in the context of the individual business relationship. What firms do to establish the nature and purpose of the business relationship can be adjusted on a risk-sensitive basis, and Title II of these guidelines contains information on what this could entail.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	Some respondents were uncomfortable with references to media searches as possible information sources and asked that these references be deleted.	The guidelines suggest a number of information sources firms can refer to when identifying the risk associated with a business relationship or occasional transaction. These include media sources, as information in the public domain can be helpful in furthering a firm's understanding of who their customers are, and in determining where further questions should be asked. The guidelines are clear that such sources should only be relied upon to the extent that they are credible and reliable. Paragraph 20 explains how firms can determine the credibility of allegations they become aware of in this way.	No change.
	Many respondents expressed strong support for the statement in paragraph 17 that firms should take a holistic view of relevant risk factors, and that isolated risk factors may not move a relationship into a higher risk or lower risk category. Some asked that this paragraph be highlighted in bold or repeated throughout the text.	This paragraph is key to the correct interpretation of these guidelines and similar statements are found throughout the text.	No change.
Customer risk factors	Several respondents commented on the beneficial ownership risk factors. They were concerned that information on beneficial owners was hard to obtain, and thought that the lesser CDD requirements in Article 13(1)(b) of Directive (EU) 2015/849 meant that fewer factors had to be considered when identifying the ML/TF risk	The guidelines do not prescribe how many risk factors firms should consider; however, firms should in any case obtain enough information on the beneficial owner to understand the risk associated with the business relationship resulting from who the beneficial owner is.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	associated with the relationship because of who the beneficial owner was. One respondent was of the view that firms should not consider the ML/TF risk associated with the beneficial owner.		
	Several respondents disagreed with suggestions that firms should consider the ML/TF risk associated with a customer's or beneficial owner's business activity.	The source of funds is an important indicator of ML/TF risk.	No change.
	Some respondents argued against the guidelines' suggestion that firms consider a customer's or a customer's beneficial owner's reputation as part of their risk assessment efforts. Poor reputation was not evidence of wrongdoing and customers should always be presumed innocent unless convicted by a court.	Understanding the reputation of those involved in the business relationship is important to assess the risk that the business relationship might be used for financial crime purposes. There is no suggestion in these guidelines that allegations of wrongdoing are evidence of criminal conduct.	No change.
	Several respondents asked that the ESAs provide guidelines on the risk associated with customers who are refugees.	The EBA issued its Opinion on the application of CDD measures to customers who are asylum seekers from higher-risk third countries or territories in April 2016, which sets out how firms can apply robust AML/CFT controls while at the same time facilitating the financial inclusion of vulnerable customers.	Explanatory detail has been added to the customer risk factors section.
Countries and geographical areas	Several respondents claimed that it was unreasonable to expect firms to assess the ML/TF risk associated with a jurisdiction; some suggested that all FATF/FSRB members should instead be deemed 'equivalent', or that the ESAs should publish a list of equivalent jurisdictions.	Directive (EU) 2015/849 requires firms to identify and assess ML/TF risk. Country risk is one of the factors firms have to consider as part of this. These guidelines set out a number of risk factors firms should consider when making that assessment. FATF mutual evaluations demonstrate that	Explanatory detail has been added to facilitate the assessment of the ML/TF risk associated with

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
		FATF/FSRB membership does not, of itself, mean that a country's AML/CFT defences are adequate.	different jurisdictions, and consequential changes have been made throughout the guidelines.
	Some respondents were concerned about references to offshore jurisdictions and tax havens. They thought these terms had unhelpful pejorative connotations and suggested that international tax cooperation was now much greater than in the past.	ML/TF risk is determined, inter alia, by a jurisdiction's commitment to international tax transparency and information sharing standards.	Explanatory detail has been added to facilitate the assessment of ML/TF risk associated with different jurisdictions, and consequential changes have been made throughout the guidelines.
Products, services and transactions risk factors	Several respondents wrote that associating non-face-to-face relationships with higher ML/TF risk conflicted with the EU's digital agenda.	Annex III to Directive (EU) 2015/849 lists non-face-to-face business relationships or transactions as potentially higher risk. In the same way, the guidelines do not suggest that non-face-to-face relationships are always high risk but instead ask firms to consider how the customer comes to the firm, which may or may not give rise to higher risk.	No change.
Weighting risk factors	Several respondents explicitly supported the statement that firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship or	This section is key to the correct interpretation of these guidelines and similar statements are found throughout the text.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	occasional transaction. This was central to a proportionate, risk-based approach and should be highlighted.		
	Several respondents explicitly welcomed the guidelines on weighting, but asked that the guidelines make clear that automated systems are not warranted in all cases.	The guidelines do not prescribe the use of automated systems, but the exclusive use of manual systems should not stand in the way of effective AML/CFT systems and controls.	This section has been amended to make clear that it only applies where firms use automated systems.
Categorising business relationships	One respondent argued that only high-risk customers needed to be categorised.	The guidelines do not prescribe how firms should categorise customers, but are clear that, in line with good risk management practices, all business relationships and occasional transactions should be categorised based on the level of ML/TF risk. Correct categorisation of business relationships is key to the application of adequate CDD and risk management measures.	No change.
SDD	Several respondents argued that the guidelines did not provide for exemptions from CDD in low-risk situations; furthermore, some respondents claimed that, in low-risk situations, beneficial owners did not need to be identified.	Directive 2005/60/EC provided for exemptions from CDD obligations in low-risk situations, subject to certain conditions. It was possible, in some cases, not to identify the beneficial owner. However, Directive (EU) 2015/849 does not provide for such exemptions. This means that firms always have to apply all CDD measures in all cases, even though the extent of these measures can be adjusted on a risk-sensitive basis.	No change.
	Several respondents complained that the guidelines' SDD section was too similar to standard CDD. There was concern, in particular, about one	In line with the FATF's Recommendations, Directive (EU) 2015/849 requires firms to apply all CDD measures in all cases. As a result, SDD measures now	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	provision suggesting that verifying identity on the basis of a single document qualified as SDD.	closely resemble CDD measures, whereas they could have resulted in exemptions under the previous regime.	
PEPs	A number of respondents felt that the guidelines' PEPs provisions were unduly onerous. Respondents took issue with the need to establish a PEP's source of wealth and source of funds, which they considered disproportionate, and several thought that requiring senior management sign-off would lead to firms avoiding business relationships with PEPs. There were suggestions that the guidelines should establish a monetary threshold below which PEP relationships were not high risk, and that the ESAs should publish PEP lists. Some respondents took issue with the guidelines' suggestion that PEP relationships did not always present the same degree of high risk, while others explicitly welcomed this as sensible and proportionate.	Article 20 of Directive (EU) 2015/849 requires firms to apply specific EDD measures to business relationships or transactions with PEPs. These EDD measures have to be applied in all cases and include the establishment of the PEP's source of wealth and source of funds, and the need for senior management approval for establishing or continuing a business relationship with a PEP. There is no exemption, in the Directive, for business relationships with PEPs that remain below a certain threshold. The Directive does, however, permit the adjustment of the extent of obligatory EDD measures on a risk-sensitive basis and the guidelines set out how this can be done.	No change.
High-risk jurisdictions and other high-risk situations	Most respondents agreed with this section but some respondents argued that information on a customer's family members or business associates should not influence the risk assessment. Others asked that the EDD measures in this section be ranked according to their importance.	In higher risk situations, information about a customer's family or close business partners can provide firms with important insights into the ML/TF risk associated with the business relationship, for example where allegations of corruption or other serious crimes exist that could increase the risk of the firm handling the proceeds of crime. It is not possible to rank EDD measures by	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
		importance as the relevance or relative importance of each measure will depend on the reason why a relationship is classed as higher risk.	
Other considerations	One respondent suggested that guidelines asking firms to terminate a business relationship where they are not satisfied that the purpose and nature of the business relationship are legitimate were not in line with Directive (EU) 2015/849. Others explicitly welcomed this provision.	The guidelines are clear that firms should enter into business relationships only where they are satisfied that they can manage the ML/TF risk. Where firms have reasonable grounds to suspect ML/TF, they must report their suspicion to the FIU.	No change.
Derisking	Several respondents welcomed guidance on derisking, although some asked that the guidelines make clear that the risk-based approach, of itself, does not require the termination of higher risk relationships and provided drafting suggestions.	This clarification is in line with the FATF's derisking statements.	This paragraph has been amended in line with respondents' drafting suggestions.
Comments on Title III			
Correspondent banking	Some respondents considered that EDD measures should not apply to correspondent relationships where banks acted in a principal-to-principal capacity.	The guidelines acknowledge that not all correspondent relationships present the same level of risk and provide guidance to firms on how to adjust their EDD measures accordingly; however, the definition of correspondent relationships in Directive (EU) 2015/849 is broad and it is not possible for these guidelines to exclude specific correspondent relationships, even if firms consider these to be associated with lower levels of ML/TF risk.	Minor amendments to better reflect different levels of high risk in line with international guidance.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	Several respondents argued that reliance on the Wolfsberg questionnaire should, of itself, be enough to meet the Directive's correspondent banking requirements.	Questionnaires are a good starting point but may not be enough to allow firms to comply with their obligations under Directive (EU) 2015/849 as transposed by Member States.	Minor amendments to clarify regulatory expectations.
Retail banking	Several respondents pointed to a perceived incompatibility between this chapter's reference to non-resident customers as potential indicators of higher risk and Directive 2014/92/EU.	Directive 2014/92/EU does not prevent the assessment of the ML/TF risk associated with a business relationship or occasional transaction and is clear that the right to open and use a basic payment account applies only to the extent that credit institutions can comply with their AML/CFT obligations.	No change.
	A clarification was requested on which CDD obligations could be met in lower risk situations by referring to a payment drawn on an account in the customer's name in an EEA country.	In lower risk situations, a payment drawn on an account in the customer's name in an EEA country may be enough to satisfy the requirements of Article 13(1)(a) and (b).	Minor amendments to clarify regulatory expectations.
	Most respondents welcomed the provisions on pooled accounts, but several asked that they be extended to apply to equivalent jurisdictions as well.	The guidelines have been amended to allow the application of SDD measures in situations where the account holder is a firm in a non-EEA jurisdiction, provided that this jurisdiction's AML/CFT regime is not less robust than the regime envisaged in Directive (EU) 2015/849 and that the firm is supervised effectively for compliance with these obligations. This provision has not been extended to other obliged entities in third countries on account of the ML/TF risk associated with obliged entities that are	Extended to equivalent countries, but only for 'firms'.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
		not firms as defined in these guidelines.	
E-money issuers	Several respondents suggested that low thresholds alone were sufficient to put an e-money product into a lower risk category.	The guidelines describe low thresholds as a factor indicating lower risk but are clear that a low threshold may not be enough to reduce terrorist financing risk. Firms have to take a holistic view of all the relevant risk factors, which, together, determine the level of ML/TF risk associated with a business relationship.	Minor changes to clarify regulatory expectations.
	One respondent was concerned that scheme-enabled cards were described as higher risk.	The ability to use an e-money product widely can give rise to higher ML/TF risk, but the guidelines are clear that firms have to take a holistic view of all the relevant risk factors that, together, determine the level of ML/TF risk associated with a business relationship.	No change.
	One respondent suggested that distributors will be unable to spot unusual multiple purchases or e-money product usage. They said that such behaviour was visible to issuers only.	There is no expectation that distributors will monitor customer behaviour after e-money has been issued. However, where a distributor who is themselves an obliged entity observes unusual behaviour at point of sale, this could indicate higher risk.	Minor changes to clarify regulatory expectations.
	One respondent asked for examples of adequate safeguards that might reduce the risk associated with non-face-to-face relationships.	Examples of adequate safeguards include electronic identification in line with Regulation (EU) No 910/2014 and anti-impersonation fraud checks.	Minor changes to clarify regulatory expectations.
	One respondent thought that issuers could not check whether a payment had been drawn on an account in the sole or joint name of the customer, and suggested that issuers should look to establish whether the customer could be shown to have	Establishing control over an account without establishing who the holder is does not meet the CDD requirements set out in Article 13(1) of Directive (EU) 2015/849.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	control over the account instead.		
	Several respondents considered that restricting the ability to reduce the intensity of ongoing monitoring to e-money products that do not exceed EUR 250 over a 12-month period was not risk-based.	Ongoing monitoring is important to understand ML/TF risk and any reduction in the intensity of ongoing monitoring has to be considered in that context. However, firms will be able to ascertain at what point transaction volumes and values cease to be low risk.	The monetary threshold has been removed.
Money remitters	A number of respondents disagreed with some higher risk indicators. These were not, of themselves, suggestive of higher ML/TF risk. Others suggested additional risk factors.	The guidelines are clear that firms should take a holistic view of relevant risk factors, and that isolated risk factors may not move a relationship into a higher risk or lower risk category.	Minor changes to clarify regulatory expectations.
	One respondent was unclear about whether the guidelines sanctioned the establishment of a business relationship or occasional transactions where CDD information was missing.	Directive (EU) 2015/849 and Regulation (EU) 2015/847 set out which information on the payer or the payee must always be obtained and verified. The guidelines recognise that many money remitters' business is primarily transaction based, and no business relationships are established. This limits what the money remitter knows about the payer or the payee, which is why this chapter sets out what a money remitter's systems should be capable of to ensure ML/TF is detected.	Minor changes to clarify regulatory expectations.
Wealth management	Several respondents suggested that it was unreasonable for wealth managers to visit the clients' location in high-risk cases.	The guidelines provide examples of EDD measures wealth managers could take in high-risk situations, but do not prescribe EDD measures. Title II of these guidelines is clear that what is appropriate will depend on the reason why a relationship was classified as high risk.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	Several respondents objected to the guidelines' suggestion that SDD was not appropriate in a wealth management context.	The application of SDD measures is reserved for low-risk situations. Annex III to Directive (EU) 2015/849 describes private banking as potentially higher risk, as the nature of wealth management, and many of the features typically associated with wealth management, are indicative of higher ML risk. This means that SDD measures are not appropriate in this context.	No change.
Life insurance	A number of respondents disagreed with various risk factors.	The guidelines are clear that firms should take a holistic view of relevant risk factors, and that isolated risk factors may not move a relationship into a higher risk or lower risk category.	No change.
Investment funds	A number of respondents asked for clarification on which party is responsible for the application of CDD measures.	The responsibility for applying CDD measures remains with the fund or the fund manager.	The guidelines have been redrafted to clarify CDD requirements in the funds distribution context.
	Several respondents considered that it was unreasonable to require investment funds to identify investors where intermediaries were used.	Directive (EU) 2015/847 is clear that firms have to identify, and verify the identity of, the customer and the beneficial owner. Beneficial owners are natural persons who own or control the customer, or on whose behalf a transaction is being conducted. The guidelines set out how funds and fund managers can meet their CDD requirements in low-risk situations.	The guidelines have been redrafted to clarify CDD requirements in the funds distribution context.