boulevard de Berlaimont 14 – 1000 Bruxelles
tél. +32 2 221 38 12
numéro d'entreprise: 0203.201.340
RPM Bruxelles
www.bnb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Communication

Public

Bruxelles, 10 octobre 2023

Référence: NBB_2023_08

vos correspondants:
Charlotte le Beau de Hemricourt / Stéphane Folie
tel. +32 2 221 56 35 / 31 41
charlotte.lebeaudehemricourt@nbb.be /
stéphane.folie@nbb.be

Analyse horizontale de contrôle consistant en l'examen d'un échantillon de transactions passées par des agents liés de différents établissements de paiement

Champ d'application

Les établissements exerçant l'activité de transferts de fonds (money remittance) et qui tombent dans le champ d'application de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces.

Résumé/Objectifs

La Banque a procédé à une analyse horizontale de contrôle consistant en l'examen d'un échantillon de transactions passées par des agents liés de différents établissements de paiement (money remitters) sous supervision. Le présent document entend formuler des points d'attention ainsi que des bonnes pratiques pour l'ensemble du secteur.

Structure

1) Supervision des agents
2) Qualité des données
3) Mesures de vigilance
4) Faits et opérations atypiques

Madame,
Monsieur,

Dans le cadre de l'exercice de ses compétences de contrôle en matière de mesures de prévention du blanchiment de capitaux et du financement du terrorisme (ci-après, « LBC/FT »), la Banque nationale de Belgique (ci-après, « la Banque ») a procédé à une analyse horizontale consistant en l'examen d'un échantillon de transactions passées par des agents liés de différents établissements de paiement actifs dans le transfert de fonds et sous supervision LBC/FT.

Sur la base des analyses réalisées et des renseignements complémentaires reçus, la Banque a constaté des bonnes pratiques mais également des lacunes dans les procédures et systèmes de contrôle de certains établissements. Celles-ci sont regroupées autour des quatre thèmes suivants: supervision des agents, qualité des données, mesures de vigilance et enfin, faits et opérations atypiques.

Vous trouverez ci-dessous le compte-rendu des principales constatations que la Banque a tirées de l'analyse susmentionnée. Des attentes et recommandations sont également formulées.

Nous adressons une copie électronique de la présente communication au(x) commissaire(s), réviseur(s) agréé(s) de votre établissement[1].

Nous vous prions de croire, Madame, Monsieur, en l'assurance de notre considération distinguée.

Pierre Wunsch
Gouverneur

[1] Si applicable.

PRINCIPALES CONSTATATIONS TIREES DE L'ANALYSE HORIZONTALE

La Banque a mené une action horizontale de contrôle consistant en l'examen de transactions passées en 2021[2] par des agents liés de différents établissements de paiement actifs dans le transfert de fonds (ci-après, « *money remitters* ») sous supervision LBC/FT. En 2018, la Banque avait déjà mené une action similaire à l'issue de laquelle la communication NBB_2018_21 avait été publiée à l'attention du secteur. La présente communication vise à compléter la précédente. Pour rappel cette première analyse avait principalement mis en évidence:

- certains cas démontrant une faiblesse dans la supervision des agents;
- la faible qualité des informations collectées relatives au client rendant dès lors difficile le monitoring adéquat des transactions;
- des scenarios post-transactionnels permettant d'identifier les schémas de type *one to many* et *many to one* appliqués sur des périodes fixes et non pas sur des périodes « flottantes », ou encore l'absence de scenarios adéquats permettant d'identifier l'activité de mules financières.

Pour mener son analyse, la Banque a sélectionné cinq établissements de paiement actifs sur le territoire belge et soumis à la supervision LBC/FT de la Banque, représentant une part de marché très significative de l'activité de « remittance » fondée sur le transfert de fonds effectués par le biais d'agents. En effet, les transactions passées par une application digitale n'ont pas fait l'objet de la présente analyse.

Pour chacun de ces établissements, la Banque a sélectionné, sur la base d'une approche fondée sur les risques, deux points de service (*i.e.* agents). La sélection a été opérée sur la base du montant moyen des transactions effectuées dans leur point de service qui les plaçait dans la fourchette haute des moyennes relevées pour l'ensemble des agents liés à l'établissement de paiement.

L'analyse a porté sur l'ensemble des transactions passées auprès de chaque point de service sélectionné durant douze mois. Il a été tenu compte d'un seuil de matérialité pour les travaux d'analyse.

Le présent document entend formuler les principaux constats et points d'attention ainsi que des bonnes pratiques pour l'ensemble du secteur.

Il peut être utilement rappelé que l'Autorité bancaire européenne a publié le 16 juin 2023 un rapport sur les risques BC/FT liés aux établissements de paiement[3] .

Les principales constatations sont regroupées autour des thèmes suivants: la supervision des agents, la qualité des données, les mesures de vigilance et les faits et opérations atypiques.

2 Il a été pris en compte les informations issues du questionnaire sur les risques inhérents communiqué à la Banque pour le 31 mai 2022 conformément à la Circulaire NBB 2022_06.

3 Report on ML TF risks associated with payment institutions.pdf (europa.eu). Outre l'indication des risques classiquement identifiés dans le secteur, il met également en lumière des risques émergeants découlant de nouveaux *business models* ou de nouvelles activités pouvant constituer une porte d'entrée du système financier pour des opérations de BC/FT.

CONSTATS ET BONNES PRATIQUES IDENTIFIES

SUPERVISION DES AGENTS

La Banque constate que certains agents sélectionnés dans l'échantillon se distinguent positivement tant par la qualité des données récoltées que par le nombre limité de transactions pouvant soulever des interrogations. Il faut y voir un lien avec la supervision des agents qui, sur la base de l'échantillon analysé par la Banque, s'est globalement améliorée tant en fréquence qu'en qualité par rapport à l'action menée en 2018. À cet égard, la Banque note toutefois des disparités importantes entre les *money remitters* d'une part, dans la profondeur et la qualité des analyses préparatoires à la visite auprès de l'agent et d'autre part, dans le suivi de la visite de l'agent dans le cadre de la mise en œuvre de la surveillance de celui-ci (ex. analyses de transactions et vérification de la qualité des données encodées).

Dès lors, compte tenu du rôle fondamental de l'agent dans le dispositif LBC/FT de l'établissement de paiement, la Banque insiste à nouveau sur l'importance de la surveillance de l'agent et du suivi qui y est apporté. Il est essentiel que les établissements de paiement déterminent et appliquent un plan de revue annuel des agents de manière à couvrir adéquatement leur réseau d'agents sur la base d'une approche fondée sur les risques.

Une bonne pratique identifiée consiste à analyser, pour l'agent contrôlé, le volume de transactions proches mais ne dépassant pas les seuils de surveillance de l'établissement. Par ailleurs, ces mesures de contrôles des agents ne doivent pas se limiter aux visites périodiques de ceux-ci. Une autre bonne pratique identifiée consiste à revoir les transactions effectuées par l'agent pour son propre compte.

QUALITE DES DONNEES

La Banque constate une amélioration significative des données d'identification des clients en comparaison avec la précédente action. L'utilisation plus développée et plus systématique du lecteur de la carte d'identité électronique (*eID*) facilite l'identification correcte du client en empêchant, entre autres, des erreurs d'encodage.

La Banque constate également que les bases de données de plusieurs *money remitters* montrent encore un certain nombre de clients enregistrés sous différents codes d'identification « uniques » (ci-après, « *ID* »). Ce multiple encodage d'un même client (« doublons ») a pour effet de compromettre les contrôles de détection basés sur le volume transactionnel en nombre et en montant enregistré pour chacun de ses identifiants uniques.

Concernant les données des bénéficiaires des clients, la Banque constate que, dans la majorité des cas, il n'existe pas de système prévenant de manière efficace l'encodage multiple d'un même bénéficiaire. Un même bénéficiaire peut dès lors se voir attribuer différents *ID* alors qu'il s'agit de la même personne. La Banque estime qu'*a minima,* lorsqu'un même client envoie des fonds à plusieurs reprises vers un même bénéficiaire, ce dernier ne devrait avoir qu'un seul *ID* dans le système du *money remitter* concerné. En effet, l'encodage multiple d'une même personne rend les contrôles basés sur la consolidation des données transactionnelles par client et/ou par bénéficiaire inefficaces

MESURES DE VIGILANCE

Le dépassement de certains seuils transactionnels, en montant ou en nombre de transactions, fixés dans les procédures de chaque établissement de paiement peut générer une alerte entraînant l'obligation de fournir des informations complémentaires, l'approbation de la transaction par la fonction compliance ou bien, le cas échéant, un blocage de la transaction. La Banque relève une grande disparité dans lesdits seuils utilisés par les *money remitters* pour déterminer les mesures de vigilance à appliquer.

Grâce à l'évaluation globale des risques établie et revue périodiquement, l'établissement doit identifier les risques auxquels il est exposé et appliquer des mesures de réduction de ces risques dont l'application de seuils appropriés. La détermination et la motivation de ces seuils doivent découler de cette analyse et doivent être dûment documentée. Des seuils trop élevés ont pour conséquence de rendre les mesures de vigilance déterminées par l'établissement dans ses procédures purement théoriques car presque jamais appliquées dans les faits. Dans ce cas, ces seuils ne sont pas des mesures de réduction des risques identifiés. La Banque invite dès lors les *money remitters* à s'assurer que les seuils utilisés sont appropriés au regard des transactions qui sont effectuées par les clients.

Concernant la période sur laquelle les seuils transactionnels sont calculés, la Banque insiste sur l'importance pour l'établissement de définir également des seuils qui se calculent sur des périodes moyennes et longues. La Banque constate en effet que la majorité des scénarios visant à identifier les schémas de type *one to many* et *many to one* sont calculés sur des périodes courtes. Il convient dès lors de complémenter ces scénarios avec des seuils adaptés sur des périodes plus longues. Ces scenarios doivent également être appliqués en « jours flottants » (ex. une transaction réalisée le 24 février est additionnée à toutes les transactions réalisées par le même client depuis le 25 janvier), mais pas sur des mois civils.

De surcroît, des seuils transactionnels ne sont pas suffisants pour déterminer les mesures de vigilance à appliquer. En effet, il convient d'établir, si ce n'est pas déjà le cas, des scénarios qui prennent en compte d'autres facteurs de risques. Afin de mettre en œuvre l'approche fondée sur les risques ainsi que d'allouer au mieux les ressources de l'établissement, les seuils transactionnels peuvent être combinés et adaptés en fonction de ces autres facteurs de risque. De manière non exhaustive, ces autres facteurs de risques peuvent être:

- le nombre de bénéficiaires du client, étant entendu que la détermination du nombre de bénéficiaires doit découler de l'évaluation globale des risques de l'établissement. Ce nombre peut donc varier selon les corridors utilisés, les origines des clients ou les caractéristiques des déclarations de soupçons faites dans le passé;
- les moyens de paiements utilisés à l'entrée et à la sortie des fonds. En effet, les transactions en cash restent plus risquées que d'autres types de transactions (ex. carte bancaire).

Par ailleurs, la Banque relève des lacunes en ce qui concerne les mesures de vigilance définies et appliquées par les *money remitters*. Elle constate que, dans la majorité des cas, seules des informations purement déclaratives sont demandées aux clients lors du dépassement de certains seuils et/ou scenarios et/ou d'un certain niveau de risque. En outre, les informations demandées au client sont génériques et limitées, et dès lors les réponses sont difficilement exploitables lors de la mise en œuvre de la vigilance. À titre d'exemple, l'origine des fonds indiquée est très souvent « le salaire » et l'occupation du client est soit « travailleur » ou « pensionné » et ce, quel que soit le montant des transactions effectuées par ce client. Qui plus est, il ressort que, parfois, les informations fournies par le client à diverses occasions sont contradictoires entre elles (ex. relation avec la contrepartie) et que ces contradictions ne soulèvent pas d'analyse approfondie *a posteriori*.

Une approche déclarative est acceptable jusqu'à un certain niveau de risque mais, passé ce niveau, il est nécessaire d'obtenir des éléments probants et une analyse circonstanciée pour corroborer les informations fournies par le client. Le niveau de risque approprié au-delà duquel des mesures de vigilances additionnelles sont nécessaires doit être déterminé, motivé et documenté par l'établissement. À nouveau, la Banque rappelle que l'évaluation globale des risques est l'élément central du disposition LBC/FT de l'établissement. Celle-ci permet d'identifier et de gérer de manière appropriée les risques inhérents en matière de BC/FT auxquels leurs activités les exposent et de mettre en œuvre les mesures de réduction de risques et les mesures de vigilance adéquates.

En lien avec ce qui est mentionné ci-dessus, la Banque constate que très peu de transactions sélectionnées par la Banque ont fait l'objet d'une analyse de la capacité financière du client, et par conséquent, de l'origine des fonds. Bien souvent, aucune analyse de la cohérence des transactions avec les revenus annoncés du client n'est faite par l'établissement, même pour des transactions significatives.

La Banque constate d'ailleurs que la collecte d'éléments probants est très exceptionnelle. Pourtant, les établissements pourraient demander et analyser les fiches de paie ou les extraits de compte prouvant le retrait en cas de paiement significatif en cash. La Banque relève à cet égard qu'il y a lieu de s'interroger sur la raison du retrait en cash en vue d'effectuer un transfert de fonds alors que les rémunérations sont systématiquement payées par virements bancaires et que les *money remitters* offrent la possibilité d'un paiement par carte. La Banque invite également les établissements à définir des critères portant sur l'antériorité maximale des documents probants qui seraient demandés au client, en particulier lorsqu'il s'agit d'extraits de compte.

À ce sujet, la Banque considère comme insatisfaisante la pratique qui consiste à se contenter de la localisation du payeur dans un « pays à revenu élevé » pour justifier la capacité économique du client à faire des transactions significatives et à se satisfaire de l'existence d'un « lien » entre le client payeur et le pays du bénéficiaire pour justifier à suffisance les transactions à destination de ce pays sans appliquer aucune mesure de vigilance.

FAITS ET OPERATIONS ATYPIQUES

Bien que la Banque constate que, globalement, la qualité de la surveillance post-transactionnelle s'est améliorée par rapport à l'action de 2018, il reste néanmoins certaines exceptions dans le secteur.

Bonnes pratiques

Avant de souligner quelques-unes des faiblesses identifiées, la Banque souhaite lister, de manière non exhaustive, certaines bonnes pratiques relevées à ce sujet.

a) La mise en place d'un scenario post-transactionnel basé sur l'adresse de résidence des clients. En effet, la Banque est d'avis qu'à partir d'un certain nombre de clients domiciliés à la même adresse, il convient de s'interroger sur le caractère atypique des transactions desdits clients et notamment sur la capacité financière de ces personnes comparées au montant cumulé de leurs transactions.
b) La mise en place d'un contrôle bloquant empêchant le client de contourner l'application des scenarios pré-transactionnels. Un client ayant initié une transaction qui a déclenché une demande d'informations complémentaires peut annuler sa transaction mais devra de toute façon fournir celles-ci lors de sa prochaine transaction, quel qu'en soit le montant ou la nature.
c) Force est de constater que le caractère « flottant » des périodes sur lesquelles les scenarios sont calculés est devenu la norme au sein du secteur. Il s'agit d'une amélioration significative par rapport à l'action menée par la Banque en 2018.

Ce type de bonnes pratiques permettent à certains *money remitters* d'identifier par exemple des réseaux suspects qui suivent des schémas de type *many to many*. Bien que ces schémas soient difficilement identifiables, certains établissements combinent plusieurs types de scenarios de surveillance leur permettant de capter ce genre de comportements. En effet, la combinaison des scenarios visant à identifier les schémas de type *one to many* et *many to one* couplée à une analyse circonstanciée et globale des transactions permettent de mettre au jour ce type de schéma. Il convient toutefois de veiller à mener les analyses et, le cas échant, de déclarer les soupçons à la CTIF dès que possible.

Points d'attention

Malgré ces améliorations, la Banque constate encore certaines lacunes qui restent relativement généralisées dans le secteur.

a) La Banque a relevé des exemples où plusieurs transactions significatives sont passées auprès d'un agent par différents clients dans un délai très court (*i.e.* quelques minutes) ce qui peut laisser penser qu'ils se sont rendus ensemble chez l'agent. Outre le caractère atypique de ces faits, il s'agit d'une pratique courante et connue pour les « mules financières ». A cet égard, la Banque souhaite réitérer ses attentes. D'une part, la Banque s'attend à ce que les agents soient formés à détecter de telles opérations et qu'ils disposent et utilisent un système de reporting

direct permettant d'alerter la seconde ligne de contrôle de l'établissement. D'autre part, la Banque s'attend à ce que des scenarios et contrôles spécifiques *ex post* soient implémentés par l'établissement. D'ailleurs, certains *money remitters* ont développé de tels scénarios permettant l'identification de transactions portant sur des montants quasi-identiques passés dans un laps de temps réduit auprès du même agent ainsi qu'un scenario détectant un client qui passe des transactions (entrantes et/ou sortantes) chez plus de deux agents différents dans un laps de temps très court.

b) La Banque invite les *money remitters* à analyser les statistiques et à élever, si nécessaire, le risque associé à certains corridors spécifiques qui seraient des « outliers » par rapport aux autres. La Banque insiste sur le fait qu'il faut pouvoir distinguer des particularités (tant le risque que l'utilisation de ce corridor spécifique) sur certaines parties de territoire pour lesquelles des anomalies statistiques seraient constatées (ex: nombre et montant moyen des transactions substantiellement supérieurs aux attentes). Cet élément peut être pris en compte lors de l'analyse des transactions dans le processus de surveillance post-monitoring (ex. analyse de l'activité de certains corridors) ainsi que dans le cadre de la surveillance des agents et la revue des transactions passées auprès des agents.

c) La Banque rappelle l'importance d'analyser les faits atypiques, en ce compris les transactions qui ne sont pas abouties ou annulées suite au déclenchement de certains seuils et/ou scenarios et donc, de mesures de vigilance. Il en va d'autant plus ainsi lorsque c'est l'établissement lui-même qui bloque une transaction pour des raisons de compliance. L'établissement doit analyser de tels faits et procéder à une déclaration d'opération suspecte, le cas échéant. Pour rappel, la Banque a indiqué de longue date sur son site internet (commentaires et recommandations de la BNB concernant la « Vigilance à l'égard des relations d'affaires et des opérations occasionnelles et détection des faits et opérations atypiques ») que doit être considéré comme un atypique le fait que "*le client renonce in extremis, de manière inopinée et sans explication crédible à l'exécution d'une opération, dès l'instant où il constate que cette exécution implique qu'il fournisse des informations démontrées quant à son identité ou à celle des bénéficiaires effectifs, qu'il révèle la finalité de l'opération ou l'origine des fonds impliqués, etc.*"

d) La Banque constate, dans un certain nombre de cas, l'absence de vigilance à l'égard des clients ayant fait l'objet d'une déclaration de soupçon à la CTIF. Pourtant, la Banque rappelle qu'un établissement ayant effectué une déclaration de soupçon est tenu de procéder à une réévaluation individuelle des risques de BC/FT, en tenant compte notamment de la particularité que le client concerné a fait l'objet d'une déclaration de soupçon et ce, afin de décider de maintenir la relation d'affaires moyennant la mise en œuvre de mesures de vigilance adaptées aux risques ainsi réévalués, ou d'y mettre fin (cf. art. 22 du règlement de la BNB du 21 novembre 2017 relatif à la prévention du blanchiment de capitaux et du financement du terrorisme.) En outre, comme l'indique le site internet de la Banque (cf. les commentaires et recommandations de la BNB concernant déclarations de soupçons, point 2.6), toute information de nature à infirmer, conforter ou modifier les éléments contenus dans une déclaration de soupçons est portée sans délai à la connaissance de la CTIF sans exigence de montant minimal et *a fortiori* lorsqu'un client procède à de nouvelles opérations suspectes.

***