REPUBLIQUE DEMOCRATIQUE DU CONGO

CELLULE NATIONALE DES RENSEIGNEMENTS FINANCIERS

CENAREF

ANALYSE STRATÉGIQUE

Tendances de blanchiment de capitaux et de financement du terrorisme dans le secteur du Mobile Money

Typologies, indicateurs et recommandations — Année 2024 -2025

Table des matières

AVANT PROPOS DU SECRÉTAIRE EXÉCUTIF **7**

I. INTRODUCTION **11**

II. CONTEXTE ET OBJECTIF **11**

III. MÉTHODOLOGIE **12**

a. Données internes CENAREF 13

b. Analyse qualitative et quantitative 13

c. Consolidation et interprétation 13

IV. TENDANCES IDENTIFIÉES **13**

A. Secteurs déclarants (incluant le type de produit impliqué dans les cas de BC/FT) 15

B. Montants impliqués dans le BC/FT dans le secteur de Mobile money 16

C. Indicateurs communs de BC 19

1. Utilisation de faux documents lors de l'ouverture et de la gestion des comptes Mobile Money 19

2. Multiples retraits par fractionnement sans justification économique 19

3. Transactions incompatibles avec le profil financier du client 20

4. Escroqueries via plates-formes frauduleuses d'investissement 20

5. Contournement des dispositions interdisant les transactions en espèces au-delà du seuil réglementaire 21

6. Convergence et simultanéité des indicateurs 21

D. Infractions sous-jacentes 22

1. Faux, usage de faux et usurpation d'identité 22

2. Escroquerie 24

3. Kidnapping (enlèvement contre rançon) 25

4. Analyse transversale des infractions sous-jacentes 25

E. Personnes impliquées (physique et morale) 26

1. Personnes physiques 27

2. Personnes morales 28

3. Analyse transversale 29

F. Secteurs des personnes morales impliquées dans le BC/FT 29

1. Secteur de la distribution de monnaie électronique 29

2. Autres secteurs impliqués 30

3. Analyse globale du risque sectoriel 31

G. Secteur d'activité des personnes physiques impliquées dans le BC/FT 31

1. Secteur de la distribution de monnaie électronique 32
2. Secteur informel et activités commerciales non structurées 33
3. Acteurs liés à des activités criminelles spécifiques 34
4. Analyse transversale des secteurs d'activité 34
5. Implications pour le dispositif LBC/FT 35
H. Produits financiers et non-financiers utilisés dans le BC/FTP 35
1. Produits financiers utilisés 36
2. Produits non-financiers utilisés 37
3. Analyse transversale des produits 38
4. Implications pour le dispositif LBC/FT 38
I. Analyse géographique 39
1. Principaux pays impliqués dans le BC/FT 39
2. Pays d'origine des fonds 40
3. Pays de destination des fonds 40
4. Analyse des flux et des risques 41
5. Implications pour le dispositif LBC/FT 41
J. Techniques de blanchiment de capitaux 42
1. Le placement des fonds illicites 43
2. L'empilement (Layering) 44
3. L'intégration 44
4. Combinaison des techniques et sophistication des schémas 45
5. Implications pour le dispositif LBC/FT 46

V. Conclusion 46

CAS ANONYMISES 48

CAS 1 : Violation des clauses contractuelles et circuit de blanchiment via Mobile Money 48
Faits 48
Analyse LBC/FT 48
CAS 2 : Escroquerie via plateformes numériques et Mobile Money 48
Faits 48
Analyse LBC/FT 49
CAS 3 : Kidnapping et paiement de rançon via Mobile Money 49
Faits 49
Analyse LBC/FT 49
CAS 4 : Faux et usage de faux dans l'ouverture de comptes Mobile Money 50
Faits 50
Analyse LBC/FT 50

CAS 5 : Usurpation d'identité et utilisation abusive des comptes Mobile Money..... 50
a. Utilisation irrégulière de comptes agents 50
b. Utilisation de comptes tiers pour dissimulation..... 51

VI. Recommandations..... 51

1. À l'attention de la CENAREF..... 51
2. À l'attention des autorités de supervision et de régulation (notamment la BCC) 52
3. À l'attention des assujettis (banques et EME) 52
4. À l'attention des autorités publiques..... 53

Ministère de l'Intérieur 53
Ministère des PTNTIC..... 53

5. Recommandations transversales 53

AVANT PROPOS DU SECRÉTAIRE EXÉCUTIF

La transformation numérique des services financiers représente une formidable opportunité pour la République Démocratique du Congo. Elle permet à des millions de personnes, y compris celles qui se trouvent éloignées des Etablissements de crédit traditionnel, d'accéder rapidement aux services de paiement, de transfert et de conservation de fonds.

Le Mobile Money est ainsi devenu un instrument incontournable de l'activité économique nationale et un puissant levier d'inclusion financière. Cependant, son importance croissante impose également une vigilance accrue. Les mêmes caractéristiques qui font son succès. La rapidité, l'accessibilité, la simplicité et la couverture géographique étendue qui constituent ses atouts peuvent être détournées par des réseaux criminels pour lever, déplacer, dissimuler, fractionner ou utiliser des fonds d'origine illicite.

La présente analyse stratégique met en évidence plusieurs risques majeurs, parmi lesquels le contournement des seuils réglementaires, les retraits fractionnés, l'utilisation de faux documents (l'usurpation d'identité), l'escroquerie, l'utilisation abusive des comptes d'agents et le recours à des transactions sans justification économique suffisante.

Les résultats obtenus nous rappellent que la lutte contre le blanchiment de capitaux et le financement du terrorisme ne peut reposer sur l'action isolée d'une seule institution. Elle exige une mobilisation collective et une coordination effective entre la CENAREF, la Banque Centrale du Congo, les établissements de monnaie électronique, les établissements de crédit, les autorités judiciaires, les services d'enquête, les administrations publiques et les autres acteurs concernés.

À travers cette publication, la CENAREF entend assurer pleinement sa mission d'analyse, d'orientation et de retour d'information. Son ambition est de mettre à la disposition des parties prenantes une connaissance plus précise des méthodes employées par les criminels, des vulnérabilités exploitées et des indicateurs susceptibles de faciliter la détection précoce des opérations suspectes.

J'invite particulièrement les établissements de monnaie électronique et les banques commerciales à renforcer leurs mécanismes de connaissance du client, de surveillance des transactions et de contrôle de leurs réseaux d'agents et de sous-agents.

La qualité des déclarations d'opérations suspectes demeure déterminante pour permettre à la CENAREF de produire un renseignement financier pertinent et exploitable par les autorités compétentes.

J'encourage également les autorités de supervision et de régulation à intensifier les contrôles fondés sur les risques, à promouvoir l'utilisation d'outils technologiques adaptés et à veiller au respect effectif des obligations légales et réglementaires applicables.

La sécurisation du secteur du Mobile Money ne doit toutefois pas avoir pour conséquence de limiter son rôle dans l'inclusion financière. Notre responsabilité collective consiste à trouver un équilibre entre l'accessibilité des services financiers, la protection des utilisateurs et la prévention de leur exploitation à des fins criminelles.

Je tiens à remercier les analystes de la CENAREF, les entités déclarantes ainsi que toutes les institutions qui ont contribué, directement ou indirectement, à la réalisation de cette étude.

Puisse ce rapport servir de référence aux professionnels, aux autorités publiques et aux décideurs, et contribuer à renforcer durablement l'efficacité et la résilience du dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Adler KISULA BETIKA YEYE

Le Secrétaire Exécutif

I. INTRODUCTION

La Cellule Nationale des Renseignements Financiers (CENAREF) a conduit la présente analyse stratégique afin de se conformer à la Recommandation 29 du GAFI, qui exige des CRF qu'elles produisent régulièrement des analyses stratégiques basées sur les informations dont elles disposent et celles reçues des autorités compétentes. Cette exigence vise à identifier les tendances, schémas, méthodes et vulnérabilités en matière de blanchiment de capitaux, de financement du terrorisme et de la prolifération des armes de destruction massive (BC/FT/PADM).

La démarche répond également à l'obligation prévue par l'article 89 de la Loi n°22/068 du 27 décembre 2022 portant lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération, telle que modifiée et complétée par la loi 25/048 du 1er juillet 2025 qui impose à la CENAREF d'assurer le retour d'informations aux assujettis et aux autorités de contrôle afin de soutenir l'efficacité du dispositif national de LBC/FT.

À travers cette étude, la CENAREF entend fournir une lecture claire et actualisée des risques émergents observés dans le secteur du Mobile Money, devenu en RDC l'un des canaux privilégiés pour les paiements, mais aussi une cible vulnérable pour les criminels financiers. Ce rapport vise ainsi à éclairer les différents acteurs : institutions financières, Établissements de Monnaie Électronique (EME), Autorités de supervision et décideurs publics, afin qu'ils renforcent leurs mécanismes de vigilance et leurs actions de prévention.

II. CONTEXTE ET OBJECTIF

L'usage massif du Mobile Money en RDC, combiné à des failles persistantes dans l'identification des clients, la traçabilité des flux et le contrôle opérationnel, a favorisé la multiplication d'infractions sous-jacentes telles que :

- l'escroquerie,
- le faux et usage de faux (l'usurpation d'identité).
- le kidnapping,

Ces pratiques criminelles ont engendré une augmentation notable des Déclarations d'Opérations Suspectes (DOS) reçues par la CENAREF en 2024, révélant des risques importants pour l'intégrité économique et financière du pays.

L'objectif de cette analyse stratégique est donc de :

- mieux comprendre les mécanismes utilisés par les criminels,
- identifier les risques et menaces spécifiques liés au secteur Mobile Money,
- évaluer les vulnérabilités des acteurs,
- orienter les mesures correctives à mettre en place,
- renforcer la contribution des assujettis à la détection des opérations suspectes,
- outiller les autorités pour une meilleure supervision basée sur les risques.

III. MÉTHODOLOGIE

La présente étude s'appuie sur une méthodologie rigoureuse, reposant sur l'exploitation des sources suivantes :

a. Données internes CENAREF

- Analyse des informations contenues dans la base de données interne ;
- Examen des DOS transmises par les banques, EME et autres assujettis ;
- Exploitation des rapports d'analyse opérationnelle finalisés en 2024.

b. Analyse qualitative et quantitative

La CENAREF a procédé à :

- l'identification des indicateurs d'alerte récurrents ;
- l'analyse des flux financiers (origine, destination, montants, produits utilisés) ;
- l'examen des profils des personnes physiques et morales impliquées ;
- l'évaluation des typologies et modes opératoires ;
- l'examen des pays d'origine et de destination des fonds ;
- la classification des cas selon les infractions sous-jacentes.

c. Consolidation et interprétation

Les informations ont été croisées afin d'obtenir :

- une vue d'ensemble cohérente des tendances émergentes ;
- une compréhension transversale des vulnérabilités ;
- une base solide pour formuler des recommandations ciblées et opérationnelles.

IV. TENDANCES IDENTIFIÉES

L'analyse des déclarations d'opérations suspectes (DOS) reçues au cours de l'année 2024 met en évidence des tendances significatives en matière de blanchiment de capitaux et de financement du terrorisme dans le secteur du Mobile Money en République Démocratique du Congo.

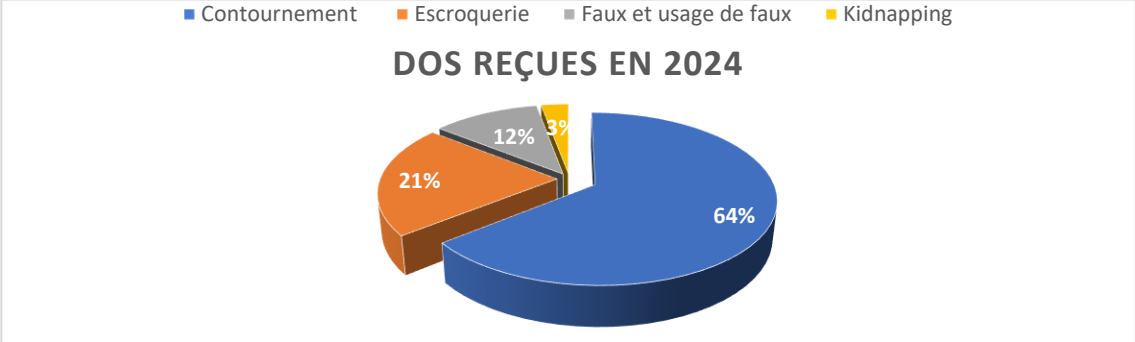
Il ressort de cette analyse que les cas de contournement des dispositions réglementaires interdisant les paiements en espèces au-delà du seuil légal constituent la tendance prédominante, représentant 64 % des DOS analysées. Cette pratique illustre une stratégie délibérée des acteurs criminels visant à exploiter les mécanismes du Mobile Money pour reconstituer des montants importants en espèces, en dehors du circuit bancaire formel.

Par ailleurs, les infractions sous-jacentes les plus fréquemment associées aux opérations suspectes sont :

- l'escroquerie, représentant 21 % des cas,
- le faux et usage de faux, à hauteur de 12 %,
- le kidnapping, représentant 3 % des cas.

Ces tendances traduisent une diversification des modes opératoires criminels, ainsi qu'une exploitation accrue des vulnérabilités du secteur du Mobile Money, notamment en matière d'identification des clients, de traçabilité des opérations et de contrôle des flux. L'ensemble de ces éléments confirme que le Mobile Money constitue aujourd'hui un vecteur à haut risque de blanchiment de capitaux, nécessitant un renforcement des mesures de vigilance et de supervision.

A. Secteurs déclarants (incluant le type de produit impliqué dans les cas de BC/FT)



Les déclarations d'opérations suspectes analysées proviennent principalement de deux catégories d'assujettis, à savoir :

- les Banques commerciales,
- les sociétés de Mobile Money, notamment les Établissements de Monnaie Électronique (EME).

L'analyse met en évidence une prédominance significative des DOS émanant des sociétés de Mobile Money, comparativement à celles transmises par les banques commerciales. Cette situation s'explique notamment par :

- la forte utilisation des services Mobile Money par une large frange de la population,
- la rapidité et l'accessibilité des transactions,
- la multiplication des points de distribution (agents et sous-agents),
- ainsi que les failles persistantes dans les mécanismes de contrôle et d'identification des clients.

En outre, les produits financiers les plus fréquemment impliqués dans les cas analysés sont :

- les transferts de monnaie électronique,
- les dépôts et retraits en espèces,
- les paiements marchands via Mobile Money,
- ainsi que les opérations de conversion entre monnaie électronique et espèces.

Ces éléments confirment que les sociétés de Mobile Money occupent une place centrale dans la détection des activités suspectes, mais également dans l'exposition aux risques de BC/FT, ce qui souligne la nécessité de renforcer leur dispositif de conformité et leurs capacités de détection.

B. Montants impliqués dans le BC/FT dans le secteur de Mobile money

Au cours de l'année 2024, le montant total identifié comme potentiellement lié à des activités de blanchiment de capitaux dans le secteur du Mobile Money s'élève à 48 905 895 USD.

Ce montant correspond exclusivement aux cas déclarés à la CENAREF et analysés dans le cadre des DOS reçues ; il ne reflète donc qu'une partie du phénomène réel, compte tenu de l'étendue du secteur, du volume de transactions quotidiennes et du degré de sous-déclaration encore observé chez certains assujettis.

La répartition des montants par tranche montre une concentration significative dans les cas de grande ampleur, ce qui démontre l'utilisation du Mobile Money non seulement pour des opérations de faible valeur mais également pour des flux financiers importants :

- De 10 000 USD à 1 000 000 USD : 3 cas identifiés

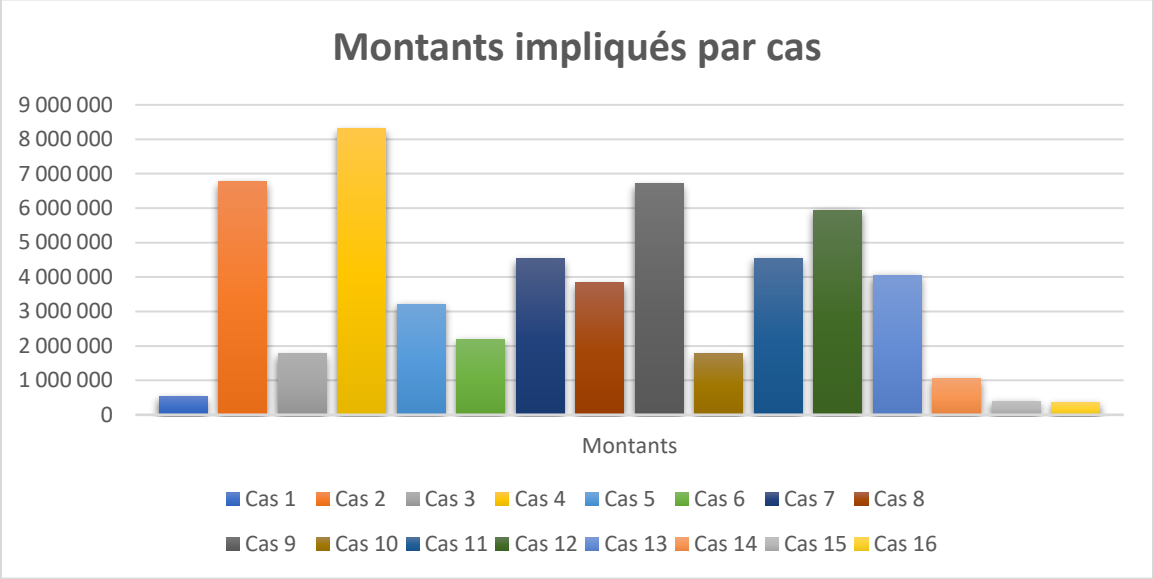
- De 1 000 001 USD à 10 000 000 USD : 13 cas identifiés

La valeur moyenne par cas est estimée à 3 056 618 USD, ce qui constitue un indicateur révélateur du niveau d'exposition du secteur et de sa vulnérabilité aux abus liés au BC/FT.

Ces montants élevés s'expliquent par plusieurs facteurs, notamment :

- le contournement des plafonds réglementaires,
- l'utilisation de comptes Mobile Money premium migrés de manière irrégulière,
- la circulation rapide de fonds entre plusieurs EME via des retraits fractionnés,
- la conversion immédiate entre espèces, monnaie électronique et comptes bancaires,
- et les flux liés à des infractions sous-jacentes telles que l'escroquerie ou les kidnappings.

L'analyse de ces montants met également en évidence que le Mobile Money est devenu un canal privilégié par les délinquants financiers, en raison de sa rapidité, de son accessibilité et des failles persistantes dans les contrôles KYC/EDD.


Montants impliqués par cas
9 000 000
8 000 000
7 000 000
6 000 000
5 000 000
4 000 000
3 000 000
2 000 000
1 000 000
0
Montants
Cas 1
Cas 2
Cas 3
Cas 4
Cas 5
Cas 6
Cas 7
Cas 8
Cas 9
Cas 10
Cas 11
Cas 12
Cas 13
Cas 14
Cas 15
Cas 16

C. Indicateurs communs de BC

L'analyse des déclarations d'opérations suspectes reçues des Établissements de Monnaie Électronique (EME) et des banques met en évidence un ensemble d'indicateurs récurrents de blanchiment de capitaux. Ces indicateurs, observés de manière simultanée dans plusieurs dossiers, témoignent d'un usage abusif et criminel des produits Mobile Money. Les principaux indicateurs identifiés sont les suivants :

1. Utilisation de faux documents lors de l'ouverture et de la gestion des comptes Mobile Money

Plusieurs clients ont utilisé des cartes d'électeurs ou des pièces d'identité falsifiées pour ouvrir des comptes ou exercer une activité de distribution de monnaie électronique.
Dans certains cas, l'absence de procédure formelle de mutation (cession d'un EME à un autre gestionnaire) favorise la circulation de comptes ouverts au nom de personnes tierces.

Impact LBC/FT :

- Masquage de l'identité réelle de l'utilisateur ;
- Difficulté de retracer les transactions suspectes ;
- Risque élevé d'usurpation d'identité et de fraude.

2. Multiples retraits par fractionnement sans justification économique

Tous les dossiers analysés font apparaître des opérations de **retraits répétitifs en petites coupures**, destinées à demeurer en dessous des seuils de contrôle définis par la réglementation.
Cette technique vise à contourner les mécanismes de vigilance des EME et à dissimuler l'ampleur réelle des flux.

Impact LBC/FT :

- Dissimulation volontaire de montants importants ;
- Indice majeur de la phase de placement dans le blanchiment ;
- Contournement manifeste des obligations de vigilance.

3. Transactions incompatibles avec le profil financier du client

Dans plusieurs cas, les montants déposés ou reçus via Mobile Money dépassent largement :

- le chiffre d'affaires déclaré,
- la capacité économique du client,
- ou l'activité commerciale renseignée lors de l'entrée en relation.

Impact LBC/FT :

- Présomption de gestion de fonds pour compte de tiers ;
- Risque élevé d'activités de blanchiment d'argent ou de financement illicite.

4. Escroqueries via plates-formes frauduleuses d'investissement

Des réseaux criminels créent des plates-formes fictives se présentant comme des sociétés connues, promettant des "investissements" à rendement rapide et élevé.

Les victimes transfèrent ainsi des fonds sur des comptes Mobile Money spécifiquement créés pour recevoir les paiements frauduleux.

Impact LBC/FT :

- Canal privilégié pour la fraude numérique ;
- Utilisation de comptes anonymes pour collecter et disperser les fonds ;

- 35 % des DOS sont liés à ces schémas d'arnaque en ligne.

5. Contournement des dispositions interdisant les transactions en espèces au-delà du seuil réglementaire

Plusieurs sociétés minières, entreprises agricoles (notamment dans le cacao) ou commerçants utilisent les services Mobile Money pour :

- transférer des montants élevés à des distributeurs de monnaie électronique,
- lesquels effectuent ensuite des retraits massifs et fractionnés,
- avant de remettre l'intégralité du cash au client final.

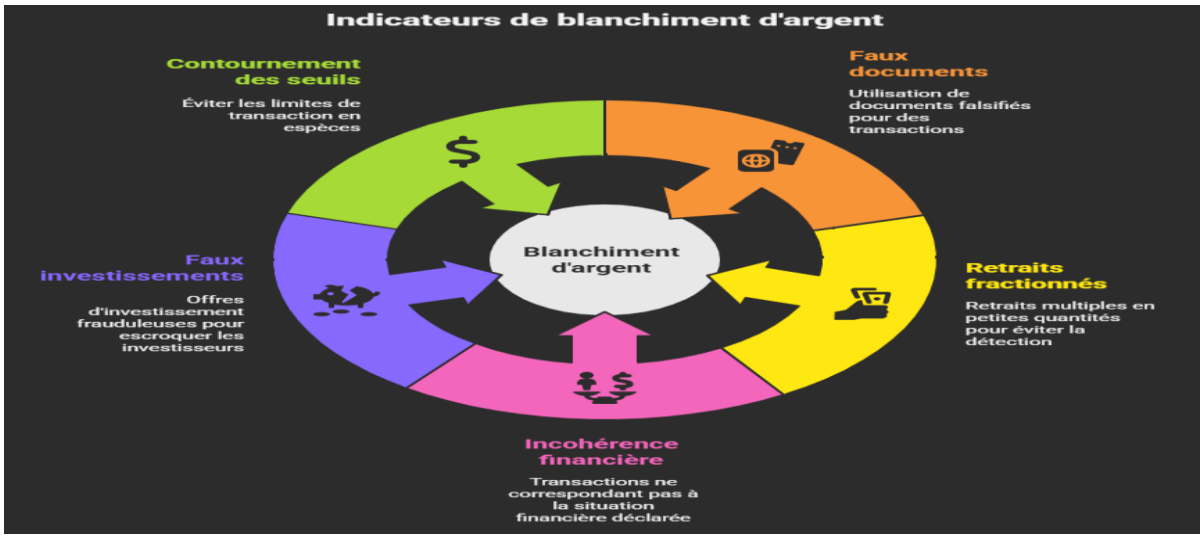
Impact LBC/FT :

- Reconstitution en espèces de montants très élevés ;
- Usage détourné des EME pour contourner l'interdiction des paiements cash ;
- Risque extrême de BC lié au commerce informel et à l'économie souterraine.

6. Convergence et simultanéité des indicateurs

Il convient de souligner que dans la majorité des dossiers, plusieurs indicateurs sont observés simultanément, notamment :

- utilisation de faux documents,
- retraits fractionnés,
- flux incohérents avec le profil du client.



Cette combinaison accroît significativement le niveau de risque et constitue un signal fort de blanchiment organisé.

D. Infractions sous-jacentes

L'analyse des déclarations d'opérations suspectes (DOS) met en évidence un ensemble d'infractions sous-jacentes prédominantes, à l'origine des flux financiers suspects observés dans le secteur du Mobile Money. Ces infractions constituent les principales sources de fonds illicites faisant l'objet d'opérations de blanchiment.

Les infractions identifiées se caractérisent par leur récurrence, leur adaptabilité aux technologies financières, ainsi que leur fort potentiel de génération de liquidités, facilitant ainsi leur intégration dans le système financier via les mécanismes de monnaie électronique.

1. Faux, usage de faux et usurpation d'identité

Description

Cette typologie constitue l'une des infractions les plus fréquemment observées dans les dossiers analysés. Elle consiste à recourir à des documents falsifiés ou à l'identité d'un tiers afin d'ouvrir, d'utiliser ou de contrôler des comptes Mobile Money destinés à réaliser des opérations financières illicites.

Elle se manifeste notamment par :

- l'utilisation de pièces d'identité falsifiées (cartes d'électeur, documents civils ou militaires) lors de l'ouverture de comptes Mobile Money ;
- l'ouverture ou l'exploitation de comptes sous de fausses identités ou des identités usurpées ;
- l'utilisation de cartes SIM enregistrées au nom de tiers ;
- l'exploitation de comptes d'agents ou de sous-agents à l'insu de leur véritable titulaire ;
- le maintien de l'exploitation d'un établissement ou d'un point de service sous l'identité de l'ancien propriétaire après une cession irrégulière.

Vulnérabilités exploitées

- insuffisance des contrôles KYC lors de l'entrée en relation ;
- absence de mise à jour des informations des clients et des agents ;
- faiblesse des mécanismes de vérification documentaire et d'authentification ;
- insuffisance des contrôles sur la propriété réelle des comptes et des comptes agents.

Impact LBC/FT

- anonymisation des flux financiers ;
- dissimulation de l'identité réelle des auteurs et des bénéficiaires effectifs ;
- complexification des enquêtes financières et du traçage des opérations ;
- détournement des circuits de distribution légitimes du Mobile Money ;

- facilitation du blanchiment de capitaux, du financement du terrorisme et d'autres activités criminelles.

2. Escroquerie

Description

L'escroquerie constitue la deuxième infraction sous-jacente la plus répandue. Elle se manifeste sous diverses formes, notamment :

- fausses plates-formes d'investissement promettant des rendements élevés ;
- annonces frauduleuses (vente de véhicules, biens de valeur, marchés fictifs) diffusées sur les réseaux sociaux ;
- exploitation de services Mobile Money pour collecter rapidement les fonds des victimes.

Dans ces schémas, les fonds sont généralement transférés vers des comptes Mobile Money, puis retirés immédiatement en espèces ou redistribués vers d'autres comptes.

Vulnérabilités exploitées

- faible niveau de sensibilisation des utilisateurs ;
- absence de contrôle sur les plate formes numériques informelles ;
- rapidité des transactions Mobile Money.

Impact LBC/FT

- génération rapide de fonds illicites ;
- difficulté de récupération des fonds ;
- multiplication des victimes et élargissement des réseaux criminels.

3. Kidnapping (enlèvement contre rançon)

Description

Le kidnapping constitue une infraction particulièrement grave, observée dans certains cas analysés. Les ravisseurs exigent le paiement de rançons via Mobile Money, en exploitant :

- la rapidité des transferts,
- la facilité d'ouverture de comptes,
- la possibilité de retirer immédiatement les fonds.

Les victimes ou leurs proches sont contraints d'effectuer des transferts vers des comptes préalablement créés à cet effet.

Vulnérabilités exploitées

- absence de mécanismes de blocage immédiat des comptes suspects ;
- difficulté de traçabilité en temps réel ;
- faible coordination opérationnelle dans certains cas.

Impact LBC/FT

- financement direct d'activités criminelles graves ;
- renforcement des réseaux criminels ;
- risque potentiel de lien avec le financement du terrorisme.

4. Analyse transversale des infractions sous-jacentes

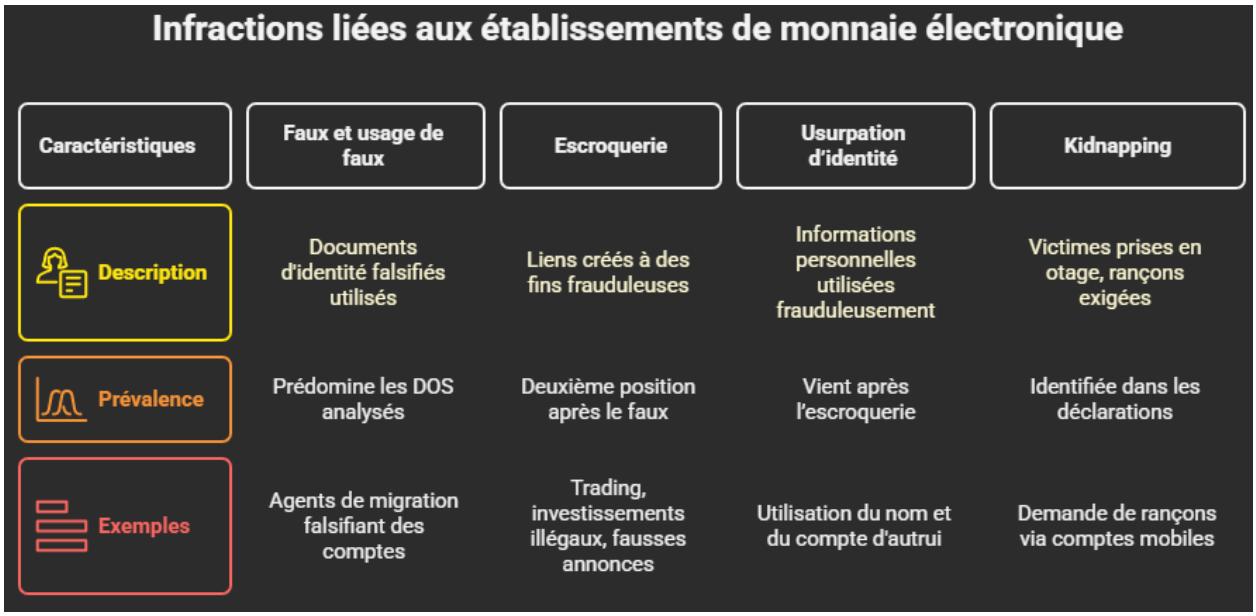
L'analyse met en évidence que ces infractions :

- sont souvent interconnectées (ex. : faux documents + escroquerie + usurpation d'identité) ;

- s'appuient sur des schémas opérationnels similaires, notamment l'utilisation de comptes Mobile Money pour collecter et disperser les fonds ;
- exploitent de manière systématique les faiblesses du dispositif de vigilance des assujettis.

Ces constats confirment que le secteur du Mobile Money est exposé à des menaces criminelles complexes et évolutives, nécessitant une approche renforcée basée sur les risques, incluant :

- un renforcement des contrôles KYC/EDD,
- une surveillance accrue des transactions,
- et une meilleure coordination entre les acteurs du dispositif LBC/FT.



E. Personnes impliquées (physique et morale)

L'analyse des dossiers traités met en évidence l'implication à parts égales de **personnes physiques et de personnes morales**, chacune représentant environ **50 % des cas analysés**. Cette répartition traduit une **structuration hybride des réseaux criminels**, combinant acteurs individuels et entités juridiques pour optimiser la dissimulation et la circulation des fonds illicites.

1. Personnes physiques

Profil général

Les personnes physiques impliquées sont majoritairement :

- des agents ou sous-agents Mobile Money,
- des opérateurs informels évoluant dans la distribution de monnaie électronique,
- des intermédiaires financiers de circonstance (prête-noms, collecteurs de fonds),
- ou encore des individus impliqués directement dans des activités criminelles (escroquerie, faux, kidnapping).

Rôle dans les schémas de BC/FT

Les personnes physiques interviennent principalement dans :

- l'ouverture de comptes (souvent avec de fausses identités),
- la réception et la dispersion rapide des fonds,
- les retraits fractionnés en espèces,
- la mise en relation entre les différents acteurs du réseau

Vulnérabilités exploitées

- faible niveau de formalisation du secteur informel ;
- insuffisance de contrôle sur les agents et sous-agents ;
- utilisation de prête-noms pour contourner les obligations de vigilance

Impact LBC/FT

- forte volatilité des flux financiers ;
- difficulté d'identification des auteurs réels ;

- fragmentation des opérations pour éviter la détection.

2. Personnes morales

Profil général

Les personnes morales impliquées comprennent principalement :

- des sociétés opérant dans la distribution de monnaie électronique,
- des entreprises commerciales (formelles ou informelles),
- des structures fictives ou écrans créées à des fins frauduleuses.

Rôle dans les schémas de BC/FT

Les personnes morales servent de :

- véhicules de transit des fonds,
- plate formes de légitimation apparente des flux financiers,
- structures facilitant les opérations de conversion (espèces ↔ monnaie électronique).

Vulnérabilités exploitées

- insuffisance de transparence sur les bénéficiaires effectifs ;
- absence de contrôle rigoureux lors de la création ou de la cession des entités ;
- faiblesse des audits internes et des dispositifs de conformité.

Impact LBC/FT

- structuration et professionnalisation des circuits de blanchiment ;
- augmentation des volumes financiers en jeu ;
- complexification des investigations financières.

3. Analyse transversale

L'implication conjointe des personnes physiques et morales met en évidence :

- une organisation structurée des réseaux criminels,
- une utilisation stratégique des personnes morales pour masquer les opérations des individus,
- une tendance à la professionnalisation des activités de blanchiment dans le secteur du Mobile Money.

Ces éléments confirment la nécessité de renforcer :

- l'identification des bénéficiaires effectifs,
- le contrôle des relations entre personnes physiques et morales,
- et les mécanismes de surveillance des agents et partenaires des EME.

F. Secteurs des personnes morales impliquées dans le BC/FT

L'analyse sectorielle des personnes morales impliquées dans les cas de blanchiment de capitaux et de financement du terrorisme met en évidence une prédominance du secteur de la distribution de monnaie électronique, qui constitue le principal vecteur d'exposition aux risques de BC/FT.

1. Secteur de la distribution de monnaie électronique

Constat

Les entités opérant dans la distribution de monnaie électronique (EME, agents et super-agents) sont les plus fréquemment impliquées dans les dossiers analysés.

Facteurs de risque

- densité élevée du réseau d'agents et sous-agents ;
- supervision opérationnelle limitée sur le terrain ;
- pratiques informelles dans la gestion des points de service ;
- cession irrégulière d'activités sans mise à jour des données.

Modes opératoires observé

- utilisation des comptes pour canaliser des fonds d'origine illicite ;
- retraits massifs et fractionnés en espèces ;
- utilisation de comptes agents pour masquer l'origine des fonds.

Impact LBC/FT

- transformation rapide de la monnaie électronique en espèces ;
- dilution de la traçabilité des flux ;
- exploitation du réseau comme canal de blanchiment.

2. Autres secteurs impliqués

Outre le secteur Mobile Money, certaines personnes morales impliquées opèrent dans :

- le commerce général,
- les activités minières artisanales,
- le négoce de produits agricoles (ex. cacao),
- ou encore des structures fictives liées à des activités frauduleuses en ligne.

Facteurs de risque

- forte circulation de liquidités ;
- faible traçabilité des transactions ;
- interactions fréquentes avec le secteur informel.

Impact LBC/FT

- injection de fonds illicites dans l'économie réelle ;
- utilisation du Mobile Money comme relais pour dissimuler les flux ;
- interconnexion entre économie formelle et informelle.

3. Analyse globale du risque sectoriel

L'ensemble des secteurs identifiés présente des vulnérabilités communes :

- insuffisance de contrôles internes ;
- faiblesse des dispositifs de conformité ;
- absence de suivi effectif des activités sur le terrain.

Ces constats appellent à :

- un renforcement de la supervision basée sur les risques,
- une meilleure régulation des agents Mobile Money,
- et une surveillance accrue des secteurs à forte intensité de cash.

G. Secteur d'activité des personnes physiques impliquées dans le BC/FT

L'analyse des dossiers met en évidence que les personnes physiques impliquées dans les opérations de blanchiment de capitaux et de financement du terrorisme évoluent principalement dans des secteurs à forte intensité de

liquidités, caractérisés par une faible traçabilité des transactions et une prédominance de l'informel.

1. Secteur de la distribution de monnaie électronique

Constat

Les personnes physiques opérant en qualité d'agents ou de sous-agents Mobile Money représentent une part significative des individus impliqués dans les cas analysés.

Vulnérabilités exploitées

- accès direct aux plate formes de transaction ;
- maîtrise des mécanismes de dépôts et retraits ;
- insuffisance de supervision effective sur le terrain ;
- possibilité d'opérer avec des identités multiples ou irrégulières.

Modes opératoires

- facilitation des retraits fractionnés en espèces ;
- utilisation de comptes agents pour canaliser des fonds illicites ;
- participation à des schémas de conversion rapide (espèces en monnaie électronique).

Impact LBC/FT

- rôle central dans la phase de placement et de dispersion des fonds ;
- affaiblissement de la traçabilité des transactions ;
- contribution à la structuration des circuits de blanchiment.

2. Secteur informel et activités commerciales non structurées

Constat

- Une proportion importante des personnes impliquées exerce dans le secteur informel, notamment :
- petits commerçants,
- opérateurs de négoce,
- intermédiaires financiers non agréés.

Vulnérabilités exploitées

- absence de formalisation des activités ;
- non-déclaration des revenus ;
- utilisation prédominante des espèces ;
- faible encadrement réglementaire.

Modes opératoires

- utilisation des comptes Mobile Money pour recevoir des fonds d'origine illicite ;
- dissimulation des flux dans des activités commerciales apparentes ;
- mélange des fonds licites et illicites (commingling).

Impact LBC/FT

- intégration progressive des fonds illicites dans l'économie réelle ;
- difficulté de distinction entre activités licites et illicites ;
- élargissement de la base des acteurs impliqués dans le blanchiment.

3. Acteurs liés à des activités criminelles spécifiques

Constat

Certaines personnes physiques impliquées sont directement liées à des infractions telles que

- escroquerie,
- faux et usage de faux,
- usurpation d'identité,
- kidnapping.

Vulnérabilités exploitées

- facilité d'ouverture de comptes Mobile Money ;
- rapidité des transactions ;
- anonymat relatif offert par les systèmes de paiement électronique.

Modes opératoires

- collecte de fonds via Mobile Money (escroquerie, rançon) ;
- retrait immédiat des fonds en espèces ;
- dispersion des montants via plusieurs comptes pour éviter la détection.

Impact LBC/FT

- génération directe de fonds illicites ;
- utilisation du Mobile Money comme canal principal de circulation ;
- renforcement des réseaux criminels.

4. Analyse transversale des secteurs d'activité

L'analyse globale révèle que les personnes physiques impliquées :

- évoluent majoritairement dans des secteurs peu régulés ou difficilement contrôlables,
- exploitent les faiblesses du dispositif de vigilance des assujettis,
- utilisent le Mobile Money comme outil central de leurs opérations financières illicites.

Ces constats mettent en évidence :

- une forte imbrication entre économie informelle et criminalité financière,
- un recours systématique à des intermédiaires pour fragmenter les opérations,
- et une tendance à la banalisation des pratiques de contournement réglementaire.

5. Implications pour le dispositif LBC/FT

Les résultats de cette analyse appellent à :

- un renforcement du contrôle des agents Mobile Money,
- une meilleure surveillance des activités informelles à risque,
- une sensibilisation accrue des acteurs économiques,
- et l'intégration d'une approche fondée sur les risques ciblant les profils les plus exposés.

H. Produits financiers et non-financiers utilisés dans le BC/FTP

L'analyse des dossiers met en évidence l'utilisation combinée de produits financiers et non-financiers, permettant aux acteurs criminels de structurer

des schémas de blanchiment efficaces, en exploitant les complémentarités entre les différents instruments.

1. Produits financiers utilisés

Les principaux produits financiers identifiés dans les cas analysés sont :

a. Dépôts et retraits en espèces

Ces opérations constituent un **point d'entrée et de sortie privilégié** des fonds illicites dans le système financier.

Rôle dans le blanchiment :

- introduction des fonds dans le système (placement) ;
- retrait des fonds après circulation (intégration/extraction).

Vulnérabilités exploitées

- contrôle limité des transactions en espèces ;
- recours aux agents Mobile Money pour fractionner les opérations.

b. Transferts de monnaie électronique (Mobile Money)

Les transferts via Mobile Money constituent le principal vecteur de circulation des fonds illicites.

Rôle dans le blanchiment :

- empilement des fonds à travers des transferts multiples ;
- dispersion des montants via plusieurs comptes.

Vulnérabilités exploitées :

- rapidité d'exécution des transactions
- multiplicité des comptes et des utilisateurs
- insuffisance de surveillance en temps réel.

c. Paiements marchands

Les paiements via Mobile Money sont parfois utilisés à des fins détournées pour donner une apparence légitime aux transactions.

Rôle dans le blanchiment :

- justification fictive des flux financiers
- intégration des fonds dans des activités commerciales apparentes.

d. Transferts nationaux et internationaux

Les flux transfrontaliers, bien que moins fréquents, participent à la **dimension internationale du blanchiment**.

Rôle dans le blanchiment :

- déplacement des fonds vers ou depuis l'étranger ;
- complexification de la traçabilité.
- **Vulnérabilités exploitées :**
- interconnexion avec des systèmes de paiement internationaux
- coordination limitée entre juridictions.

2. Produits non-financiers utilisés

a. Actifs virtuels (cryptomonnaies)

Bien que non réglementées en République Démocratique du Congo, les cryptomonnaies ont été identifiées dans certains cas comme un outil complémentaire de dissimulation des fonds.

Rôle dans le blanchiment :

- transfert de valeur hors du système financier classique ;
- anonymisation partielle des transactions.

Vulnérabilités exploitées :

- absence de cadre réglementaire ;
- difficulté de traçabilité des transactions.

3. Analyse transversale des produits

L'utilisation combinée de ces produits permet aux criminels de mettre en œuvre un schéma complet de blanchiment :

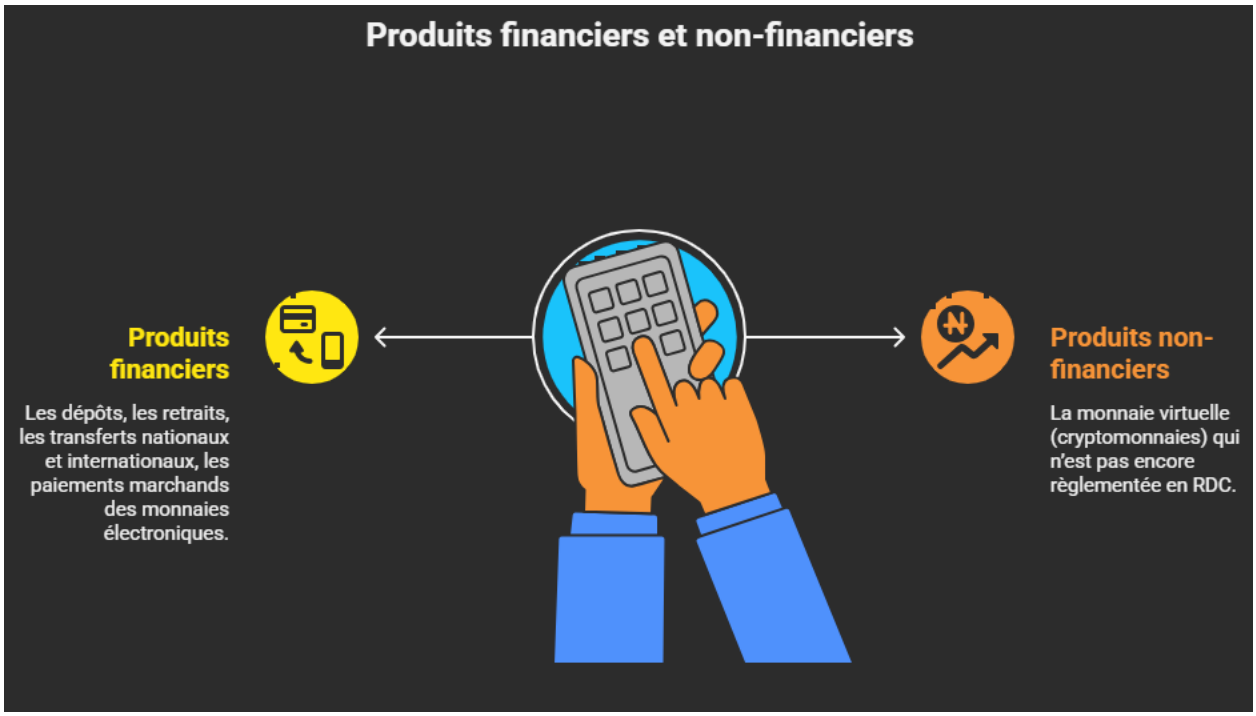
- Placement : dépôts en espèces et conversion en monnaie électronique ;
- Empilement : transferts multiples via Mobile Money et comptes intermédiaires ;
- Intégration : retraits en espèces ou utilisation via paiements marchands.

Cette complémentarité renforce la **résilience des schémas criminels** et complique leur détection.

4. Implications pour le dispositif LBC/FT

Ces constats appellent à :

- un renforcement de la surveillance des transactions en espèces ;
- une amélioration des systèmes de détection des transactions atypiques ;
- une régulation progressive des actifs virtuels ;
- une coordination accrue entre les acteurs financiers et les autorités.



I. Analyse géographique

L'analyse géographique des flux financiers met en évidence des **dynamiques nationales et internationales**, traduisant l'existence de circuits de blanchiment structurés et interconnectés.

1. Principaux pays impliqués dans le BC/FT

Les flux internationaux identifiés impliquent principalement les pays suivants :

- États-Unis,
- France,
- Cameroun,
- Nigéria,
- Côte d'Ivoire,
- Australie,
- Royaume-Uni,

- ainsi que la République Démocratique du Congo.

Ces flux transitent généralement via des messageries financières internationales en interaction avec les plate formes de Mobile Money.

2. Pays d'origine des fonds

L'analyse révèle que la RDC constitue le principal pays d'origine des fonds, suivie par certains pays étrangers, notamment :

- la Chine,
- la France,
- les Émirats Arabes Unis,
- l'Allemagne,
- Hong Kong,
- l'Inde,
- le Tadjikistan.

Analyse

Cette configuration indique :

- une forte production domestique de fonds illicites,
- combinée à des apports financiers transnationaux, souvent liés à des activités commerciales ou frauduleuses.

3. Pays de destination des fonds

La République Démocratique du Congo apparaît comme le principal pays de destination des fonds, ce qui traduit :

- une tendance à la réintégration des fonds dans l'économie nationale,
- une utilisation du Mobile Money comme canal de distribution locale.

4. Analyse des flux et des risques

Constats majeurs

- prédominance des flux nationaux, avec une forte concentration en RDC ;
- existence de flux transfrontaliers, contribuant à la complexité des schémas ;
- utilisation de canaux hybrides combinant Mobile Money et systèmes internationaux.

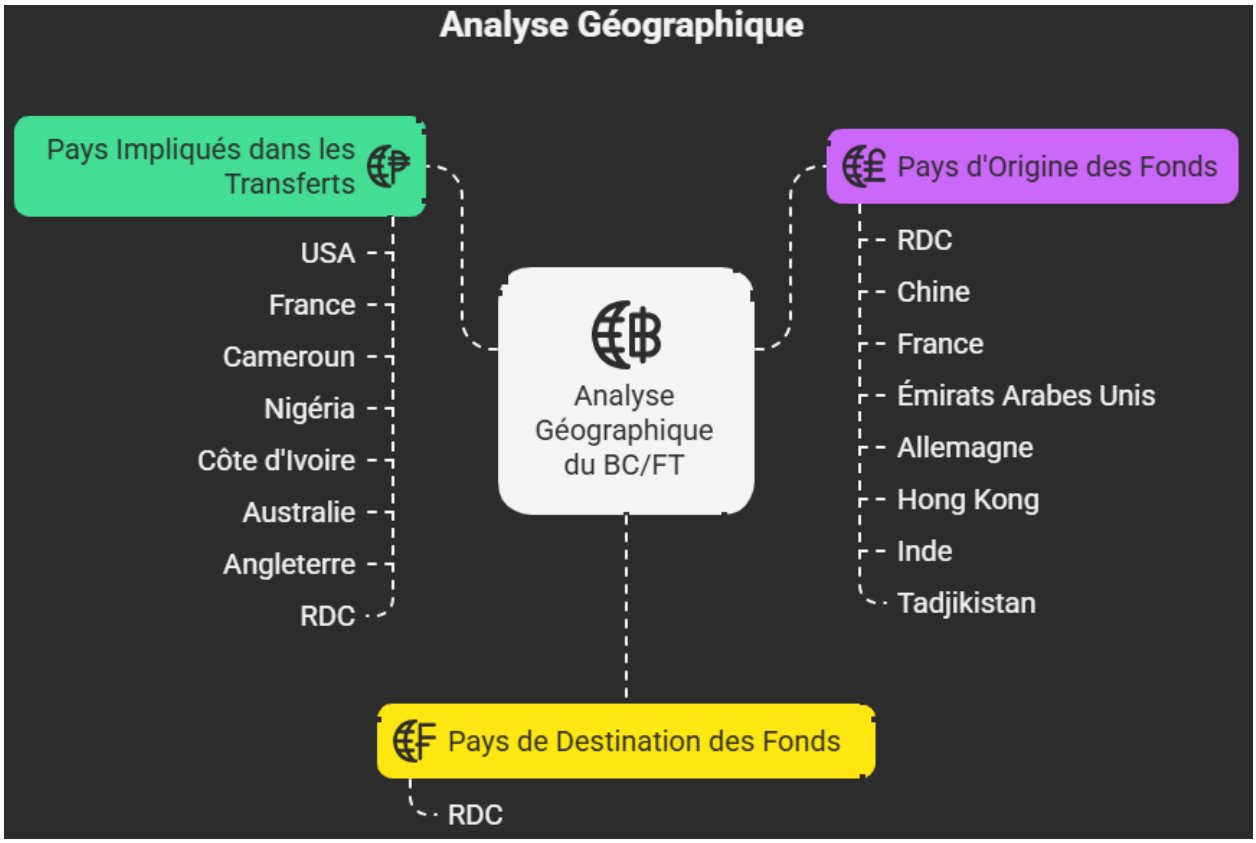
Risques identifiés

- difficulté de traçabilité des flux internationaux ;
- risque de transfert de fonds liés à des activités criminelles organisées ;
- potentiel lien avec des réseaux de financement illicite transnational.

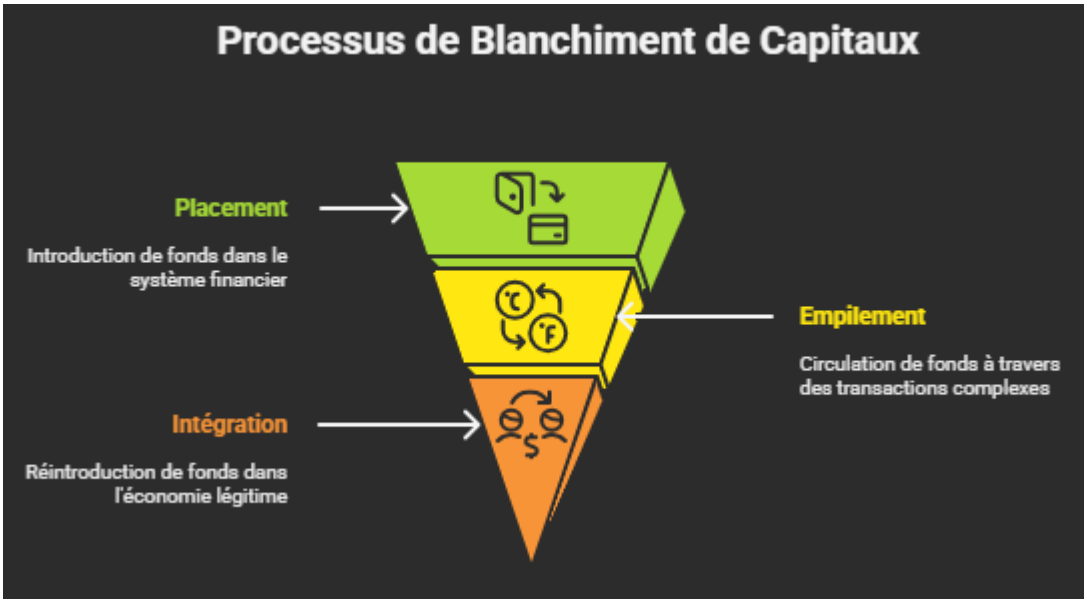
5. Implications pour le dispositif LBC/FT

L'analyse géographique met en évidence la nécessité de :

- renforcer la coopération internationale entre cellules de renseignement financier ;
- améliorer la surveillance des flux transfrontaliers ;
- développer des mécanismes d'échange d'informations en temps réel ;
- intégrer une approche géographique dans l'évaluation des risques nationaux.



J. Techniques de blanchiment de capitaux.



L'analyse des dossiers met en évidence l'utilisation systématique des trois phases classiques du blanchiment de capitaux, à savoir le placement,

l'empilement (layering) et l'intégration, dans des schémas adaptés aux spécificités du secteur du Mobile Money.

Ces techniques sont souvent utilisées de manière combinée et simultanée, ce qui complexifie la détection des flux illicites et renforce la résilience des réseaux criminels.

1. Le placement des fonds illicites

Description

Le placement constitue la première étape du processus de blanchiment, consistant à introduire des fonds d'origine illicite dans le système financier.

Modes opératoires observés

- dépôts en espèces sur des comptes Mobile Money ou bancaires ;
- conversion de fonds en monnaie électronique via des agents ;
- utilisation de comptes ouverts sous de fausses identités ou des identités usurpées ;
- fragmentation des dépôts pour éviter les seuils de déclaration.

Vulnérabilités exploitées

- contrôle insuffisant des opérations en espèces ;
- défaillances dans les procédures KYC ;
- supervision limitée des agents Mobile Money.

Constat clé

Le placement a été identifié dans 100 % des dossiers analysés, ce qui confirme son caractère systématique dans les schémas observés.

2. L'empilement (Layering)

Description

L'empilement vise à dissimuler l'origine des fonds en multipliant les transactions afin de rompre le lien avec l'infraction sous-jacente.

Modes opératoires observés

- transferts successifs entre plusieurs comptes Mobile Money ;
- utilisation de comptes appartenant à des tiers (prête-noms) ;
- fractionnement des fonds en plusieurs opérations de faible montant ;
- combinaison de flux entre Mobile Money, comptes bancaires et espèces.

Vulnérabilités exploitées

- rapidité et instantanéité des transactions ;
- multiplicité des comptes et des canaux ;
- insuffisance de surveillance en temps réel

Impact

- complexification de la traçabilité ;
- dilution de l'origine des fonds ;
- difficulté d'identification des bénéficiaires effectifs.

3. L'intégration

Description

L'intégration consiste à réintroduire les fonds blanchis dans l'économie légale, en leur donnant une apparence licite.

Modes opératoires observés

- retraits massifs en espèces via des agents Mobile Money ;

- utilisation des fonds dans des activités commerciales apparentes ;
- paiements marchands fictifs pour justifier les flux ;
- réinvestissement dans des secteurs à forte intensité de cash.

Vulnérabilités exploitées

- faible contrôle des activités économiques informelles ;
- insuffisance de vérification de la cohérence économique des transactions ;
- absence de suivi des bénéficiaires effectifs.

Impact

- insertion des fonds illicites dans l'économie réelle ;
- renforcement de l'économie informelle ;
- difficulté de détection a posteriori.

4. Combinaison des techniques et sophistication des schémas

L'analyse révèle que les trois phases du blanchiment sont présentes dans l'ensemble des dossiers étudiés, ce qui traduit :

- une maîtrise des techniques de blanchiment par les acteurs criminels,
- une adaptation des méthodes aux spécificités du Mobile Money,
- une sophistication croissante des schémas utilisés.

Les criminels exploitent particulièrement :

- la rapidité des transactions électroniques ;
- la facilité d'accès aux services financiers ;
- les failles dans les dispositifs de contrôle.

5. Implications pour le dispositif LBC/FT

Ces constats mettent en évidence la nécessité de :

- renforcer les contrôles à l'entrée en relation (KYC/EDD) ;
- améliorer la surveillance des transactions en temps réel ;
- développer des outils d'analyse permettant d'identifier les schémas complexes de transactions ;
- intensifier la coordination entre les assujettis et les autorités compétentes ;
- promouvoir une approche fondée sur les risques ciblant les phases critiques du blanchiment.

V. Conclusion

L'analyse des tendances de blanchiment de capitaux et de financement du terrorisme dans le secteur du Mobile Money en République Démocratique du Congo met en évidence une exposition élevée et croissante du secteur aux risques de criminalité financière.

Le Mobile Money, en raison de sa large accessibilité, de la rapidité des transactions et de l'importance de son réseau de distribution, constitue à la fois un levier d'inclusion financière et un vecteur privilégié d'exploitation par les acteurs criminels.

Les résultats de cette étude démontrent notamment :

- une prédominance des schémas de contournement des seuils réglementaires, à travers des retraits fractionnés et la reconstitution de liquidités ;

- une forte implication des infractions sous-jacentes telles que l'escroquerie, le faux et usage de faux, et le kidnapping ;
- une utilisation systématique et combinée des trois phases du blanchiment (placement, empilement, intégration) ;
- une imbrication étroite entre économie formelle et informelle, rendant la traçabilité des flux plus complexe ;
- un rôle central des agents et réseaux de distribution Mobile Money, à la fois dans la détection et dans l'exposition aux risques.

En outre, l'analyse met en évidence une capacité croissante des acteurs criminels à adapter leurs méthodes, en exploitant les failles opérationnelles et réglementaires du dispositif, ainsi que les évolutions technologiques.

Ces constats confirment que le secteur du Mobile Money constitue un enjeu stratégique majeur pour le dispositif national de LBC/FT, nécessitant une réponse coordonnée, proportionnée et fondée sur les risques.

Le secteur de Mobile Money a joué un rôle prédominant dans la détection d'activités de blanchiment de capitaux et de financement du terrorisme. Par ailleurs, les déclarations du secteur bancaire n'ont pas pu identifier beaucoup des cas d'activités terroristes en rapport avec le secteur de Mobile money.

Les différents cas analysés dans le secteur de Mobile money au cours de l'année 2024 a relevé un montant global de 48.905.895 USD.

Ces fonds proviennent principalement de la fraude sous diverses formes entre autres escroquerie et kidnapping. Cependant les transactions sans justifications économiques sont les indicateurs communs les plus identifiés.

Les personnes impliquées sont majoritairement de nationalité congolaise, la RDC vient en première position comme pays d'origine et de destination des fonds identifiés.

CAS ANONYMISES

CAS 1 : Violation des clauses contractuelles et circuit de blanchiment via Mobile Money

Faits

Un établissement opérant sous le statut de Marchand Indépendant auprès d'un Établissement de Monnaie Électronique (EME), censé exercer dans la restauration, n'a enregistré aucune activité commerciale réelle sur son compte Mobile Money entre février et octobre 2024.

En revanche, l'analyse de ses comptes bancaires a révélé d'importants flux créditeurs en espèces, s'élevant à :

- 2.978.272.840 CDF,
- 1.125.256 USD.

Ces fonds ont été convertis en dollars américains, puis :

- partiellement retirés en espèces,
- partiellement convertis en monnaie électronique, avant d'être transférés vers un autre EME pour des retraits systématiques.

Analyse LBC/FT

- activité déclarée fictive ;
- utilisation du Mobile Money comme canal de conversion et de retrait de fonds ;
- contournement des clauses contractuelles (paiement marchand fictif).

CAS 2 : Escroquerie via plateformes numériques et Mobile Money

Faits

Un individu nommé ZACHARIE a usurpé l'identité du Directeur Général de la douane en diffusant sur les réseaux sociaux des annonces frauduleuses relatives à des ventes aux enchères fictives.

Les victimes ont été invitées à verser des montants de **100 à 200 USD** via Mobile Money.
Le montant total collecté est estimé à **4 000 USD**, immédiatement retiré en espèces auprès d'un agent mobile money .

Analyse LBC/FT

- exploitation de la crédibilité d'une autorité publique ;
- utilisation du Mobile Money comme outil de collecte rapide des fonds ;
- retrait immédiat empêchant toute récupération.

CAS 3 : Kidnapping et paiement de rançon via Mobile Money

Faits

Une victime a été enlevée par un groupe criminel, qui a exigé le paiement d'une rançon de 5 000 USD via Mobile Money.
Les ravisseurs ont transmis aux proches de la victime :

- des images,
- des menaces,
- et un numéro de compte Mobile Money destiné à recevoir les fonds.

Analyse LBC/FT

- utilisation du Mobile Money pour le paiement de rançons ;
- rapidité de transfert et retrait des fonds ;
- difficulté de traçabilité en temps réel.

CAS 4 : Faux et usage de faux dans l'ouverture de comptes Mobile Money

Faits

Un individu a utilisé une fausse identité pour ouvrir un compte auprès d'un EME, qu'il a ensuite utilisé pour effectuer des opérations d'achat de monnaie électronique.

Des vérifications menées par l'EME ont permis de détecter l'irrégularité (pour faux et usage de faux), entraînant la rupture de la relation d'affaires.

Analyse LBC/FT

- contournement des procédures KYC ;
- utilisation d'identités fictives pour opérer dans le système ;
- risque élevé d'anonymisation des flux.

CAS 5 : Usurpation d'identité et utilisation abusive des comptes Mobile Money

a. Utilisation irrégulière de comptes agents

Faits

Un individu exploite les SIM et comptes Mobile Money d'un établissement et de ses sous-agents, pour effectuer des transactions, sans mutation légale après cession.

Analyse LBC/FT

- absence de mise à jour des titulaires ;
- difficulté d'identification du véritable opérateur ;
- traçabilité compromise.

b. Utilisation de comptes tiers pour dissimulation

Faits

Un commerçant expatrié a utilisé les comptes Mobile Money d'un établissement et de ses agents pour effectuer des opérations atypiques.

Analyse LBC/FT

- utilisation de comptes tiers pour masquer l'origine des fonds ;
- dissociation entre utilisateur réel et titulaire du compte ;
- complexification des investigations financières.

VI. Recommandations

Au regard des vulnérabilités identifiées et des tendances observées, les recommandations suivantes sont formulées afin de renforcer l'efficacité du dispositif national de lutte contre le BC/FT :

1. À l'attention de la CENAREF

- Renforcer la production et la diffusion d'analyses stratégiques ciblées, notamment par secteur et par typologie, afin d'améliorer la compréhension des risques par les assujettis ;
- Développer des indicateurs d'alerte spécifiques au Mobile Money, intégrés dans les outils de détection des assujettis ;
- Intensifier les actions de retour d'information (feedback) à l'endroit des entités déclarantes pour améliorer la qualité des DOS ;
- Promouvoir l'utilisation de solutions technologiques avancées (data analytics, scoring de risque) pour identifier les schémas complexes de blanchiment ;

- Renforcer la coopération nationale et internationale, notamment avec les CRF étrangères, en matière d'échange d'informations.

2. À l'attention des autorités de supervision et de régulation (notamment la BCC)

- Renforcer la supervision basée sur les risques des Établissements de Monnaie Électronique (EME) et de leurs réseaux d'agents ;
- Mettre en place des contrôles réguliers et ciblés sur les activités des agents et sous-agents Mobile Money ;
- Exiger l'implémentation de dispositifs robustes de KYC et de connaissance du bénéficiaire effectif ;
- Encadrer strictement les conditions de cession et d'exploitation des points de service Mobile Money ;
- Développer un cadre réglementaire adapté pour les actifs virtuels et les nouveaux moyens de paiement.

3. À l'attention des assujettis (banques et EME)

- Renforcer les dispositifs de vigilance à l'entrée en relation (KYC) et de mise à jour des données clients ;
- Mettre en place des systèmes de surveillance automatisée des transactions, capables de détecter les opérations fractionnées et atypiques ;
- Améliorer la qualité et la pertinence des déclarations d'opérations suspectes (DOS) ;
- Former régulièrement le personnel à la détection des indicateurs de BC/FT, notamment dans le contexte du Mobile Money ;
- Effectuer des contrôles périodiques sur le terrain pour vérifier la conformité des agents ;

- Suspendre ou résilier les relations d'affaires présentant des risques avérés.

4. À l'attention des autorités publiques

Ministère de l'Intérieur

- Accélérer le processus d'identification de la population afin de réduire les risques liés à l'utilisation de fausses identités.

Ministère des PTNTIC

- Mettre en place des mécanismes de surveillance et de contrôle des plateformes numériques, notamment celles utilisées à des fins d'escroquerie.

5. Recommandations transversales

- Développer une approche nationale coordonnée fondée sur les risques, intégrant l'ensemble des parties prenantes ;
- Renforcer la sensibilisation des utilisateurs des services Mobile Money aux risques de fraude et de blanchiment ;
- Promouvoir la formalisation progressive du secteur informel ;

Mettre en place des mécanismes de traçabilité renforcée des transactions en espèces ;

- Intégrer le secteur du Mobile Money comme priorité dans les évaluations nationales des risques (ENR).