BIENVENUE À LA FORMATION SUR LA CONFORMITE

PRESENTEE PAR
MADAME HAYATTI HAMADI
& MOHAMED ELAMINE MZE

SAMEDI 1ER JUIN 2024

A L'HOTEL LE RITAJ


MERCI
D'ETEINDRE
VOS TELEPHONES

Les exigences de la SNPSF en matière de Conformité

FORMATION DES AGENTS AFFECTES DANS LES SERVICES DE TRAITEMENT DE TRANSACTIONS

TABLE DES MATIERES

Les exigences de la SNPSF en matière de Conformité

INTRODUCTION

Introduction (1/3)

Qu’est ce que la Conformité?

- Les institutions financières peuvent servir, **sans le savoir, d'intermédiaires pour les activités illégales.**

- **La Conformité** existe pour satisfaire aux exigences légales promulgué par les gouvernements dans leur lutte contre les crimes financiers tels que le blanchiment d’argent, le financement du terrorisme, la fraude, la traite des êtres humains et tout autre activités criminelles.

- Ainsi, **la Conformité est le respect des lois et des réglementations en vigueur, les standards professionnels/éthiques et les procédures internes** tels que définis par La politique de conformité des partenaires à l’échelle mondiale.

Introduction (2/3)

Qu’est ce que la Fraude/le Blanchiment d’argent/le Financement du Terrorisme?

Dans un contexte où les menaces criminelles sont croissantes, les institutions financières doivent empêcher les activités illégales et atténuer les risques auxquels elles sont exposées tels que :

- **La Fraude**, c’est-à-dire vol d’informations et de fonds auprès d’agents et/ou de clients au moyen de tromperies, de tromperies, de manipulations ou d’autres moyens illégaux.

- **Le Blanchiment d’argent**, c’est-à-dire lorsque des criminels « blanchissent » illégalement de l’argent acquis. Afin de cacher la véritable source des fonds, ils placent leurs fonds dans le système financier légal et achètent des actifs légitimes/légaux (placement – superposition – intégration) par le biais de transferts d’argent, de cartes prépayées, de paiements de factures, etc.

- **Le Financement du terrorisme**, c’est-à-dire lorsque des criminels utilisent des fonds obtenus légalement ou illégalement pour commettre un acte terroriste. Lorsque les fonds sont obtenus légalement, ce processus est appelé « noircissement de l’argent ».

- **Dans le cas de blanchiment d’argent** et de **financement du terrorisme**, les criminels utilisent des techniques pour échapper à l’attention des autorités et pour protéger l’identité de leurs commanditaires et des bénéficiaires ultimes des fonds.

Introduction (3/3)
Pourquoi la conformité est-elle importante?

- D'importantes pénalités continuent d'être imposées aux dirigeants des institutions financières. La conformité est donc un élément essentiel pour la SNPSF car elle contribue à gérer les risques liés aux crimes financiers et à protéger la réputation de la banque et de la poste.

- De plus, la conformité contribue à rétablir la confiance du marché et à créer un contexte qui favorise le développement commercial.

- Le non-respect des exigences en matière de conformité peut entraîner :
  - Des dommages à la réputation;
  - Des pénalités financières et des amendes;
  - La suspension/résiliation du contrat avec nos partenaires tel que WesterneUnion ;
  - Des peines d'emprisonnement (les agents peuvent être tenus personnellement responsables des infractions).

Les exigences de la SNPSF en matière de Conformité

PARTIE 1 :
POLITIQUES ET PROCÉDURES INTERNES DE LA SNPSF EN MATIÈRE DE CONFORMITÉ

Une bonne conformité est une bonne affaire !

La réputation en matière d'intégrité de la SNPSF est essentielle à son succès.

Qui est concerné par la Conformité ?

La conformité s'applique à tous les **employés de la SNPSF** (peu importe leurs statuts incluant les salariés à temps partiel, et les stagiaires) travaillant au sein de la SNPSF et concerne toutes les activités de la banque et de la poste.

Non-respect de la Conformité ou des exigences réglementaires

Le non-respect :

- Des obligations légales applicables aux activités de la SNPSF ;
- Des exigences gouvernementales, réglementaires ou du marché, applicables aux activités de la SNPSF ; ou
- Du manuel de Conformité de la SNPSF

Peut entraîner l'une ou plusieurs des actions suivantes listées :

1. **Mesures disciplinaires prises par l'institution :** La SNPSF peut réprimander ou congédier les employés qui ne respectent pas les règles des autorités externes en vigueur.
2. **Mesures disciplinaires prises par les autorités :** Les autorités réglementaires (BCC, tribunaux etc.) peuvent également prendre des mesures d'ordre financier et sanctionner les particuliers et les entreprises qui enfreignent les réglementations en vigueur.
3. **Expulsion d'une personne :** Les autorités peuvent prendre des mesures pour mettre fin à la titularisation d'un employé et ainsi, interdire à la personne d'exercer une activité professionnelle dans le secteur financier.
4. **Litige :** Tout client qui croit avoir subi une perte peut prendre des mesures contre la SNPSF et/ou l'employé, pour obtenir une indemnisation.
5. **Poursuites pénales :** Dans certaines circonstances, les organismes gouvernementaux ainsi que les clients peuvent intenter une action en justice contre la SNPSF et/ou contre les employés.

Objectifs des politiques et procédures internes

1. Protéger la SNPSF contre le fait d'être utilisée comme un accès au blanchiment d'argent et au financement du terrorisme.

2. Implémenter des politiques et procédures de «Connaissance des clients (KYC)» pour tous les clients particuliers de la SNPSF, les entreprises et les institutions.

3. Prendre les mesures nécessaires pour détecter les activités inhabituelles ou suspectes et émettre une déclaration de soupçon, une fois celles-ci identifiées, à la Banque Centrale des Comores (BCC) conformément à la réglementation en vigueur.

4. S'engager à appliquer pleinement les lois en vigueur en matière de lutte contre le blanchiment d'argent et de financement du terrorisme ainsi que les instructions et procédures réglementaires émises par la Banque Centrale des Comores (BCC), en plus des recommandations émises par le GAFI (Groupe d'action financière) liées à la lutte contre le blanchiment d'argent.

Scope des politiques et procédures internes

1. La loi 12-008/AU, portant lutte contre le blanchiment d'argent et le financement du terrorisme en Union des Comores ;

2. Les Initiatives internationales de lutte contre le blanchiment d'argent et le financement du terrorisme.

3. Les recommandations émises par le GAFI (Groupe d'action financière) s'agissant des procédures financières et de l'élaboration d'actions conjointes des institutions gouvernementales pour améliorer et renforcer les procédures de lutte contre le blanchiment d'argent.

4. Le manuel des procédures de la SNPSF.

5. Le tableau de bord de la cartographie des risques de la SNPSF.

6. Le manuel de conformité du programme LCB/FT de la SNPSF.

La Politique de conformité de la SNPSF et de ses sous-agents opérationnels établit le cadre permettant d'identifier, d'évaluer, de contrôler, de surveiller et de signaler les risques de conformité dans l'ensemble de l'organisation afin de réduire le risque lié aux activités de blanchiment d'argent, de fraude et de financement du terrorisme.

- Les clients sont communément définis comme étant la « ligne zéro » de défense dans la protection des clients. Ils sont responsables de leurs propres transactions. Ils sont souvent les premiers informés d'une irrégularité sur leur compte.

- Les employés de la SNPSF ainsi que les sous-agents opérationnels sont la première ligne de défense. Ils sont en charge d'identifier les processus et procédures susceptibles de présenter des insuffisances en matière de protection des clients et d'escalader ces cas à la direction de leur Service ou de les signaler directement au responsable de la conformité.

- La direction des risques et de la conformité est la deuxième ligne de défense.

- La fonction Audit Interne constitue la troisième ligne de défense.

Les exigences de la SNPSF en matière de Conformité

PARTIE 2 :
EXIGENCES EN MATIÈRE DE TRAITEMENT DES TRANSACTIONS

Pour s'acquitter de leurs obligations réglementaires, les agents et sous-agents affectés dans les Services de traitement de transactions à la SNPSF doivent effectuer, pour toutes les transactions, les actions suivantes :

- **Recueillir** divers types **d'information** tout au long du processus de traitement de la transaction, notamment :
  - L'identification des clients avant le traitement de la transaction, conformément aux exigences locales et aux exigences de nos partenaires tel que MoneyGram;
  - L'information provenant des documents requis;
  - Les informations comportementales/non verbales (lorsque les transactions sont effectuées en personne), telles que le langage corporel et le ton de la voix.

- **Recueillir et saisir des informations complètes, correctes, cohérentes et exactes** sur l'identification des clients dans le système d'information requis à cet effet, afin d'assurer la qualité des données et de minimiser les retards dans le traitement de la transaction.

- Demander le numéro de référence au client et entrer ce numéro dans le systèmes d'information (ex. MoneyGram) avant de transférer les fonds au client.

- **Conserver les dossiers liés aux transactions**, les dossiers de due-diligence relatifs aux clients et tous les documents concernant la formation, le contrôle des transactions et la production de rapports en matière de conformité, dans un endroit sûr pendant au moins 5 ans, comme l'exige la réglementation locale.

- **Avertir les clients des cas de fraudes potentiels** avant la réalisation de leur transaction en faisant référence aux avertissements sur le formulaire d'envoi (le cas échéant) ou à d'autres renseignements pertinents sur les produits et en refusant de traiter les transactions potentiellement liées à la fraude.

- Maintenir des exigences transactionnelles minimales avant le traitement de la transaction. MoneyGram exige des agents qui traitent en moyenne au moins cinquante (50) transactions par mois au cours d'une période de six mois.

Ne pas traiter les transactions des clients de moins de 18 ans!

Les exigences de la SNPSF en matière de Conformité

PARTIE 3 :
EXIGENCES EN MATIÈRE D'IDENTIFICATION ET DE VÉRIFICATION DE L'IDENTITÉ DES CLIENTS

Partie 3.1 : Exigences en matière d'identification et de vérification de l'identité des clients

- **Au minimum, les informations complètes, correctes, cohérentes et exactes suivantes sont à vérifier par les agents :**
  - Nom complet du client tel qu'il apparaît sur sa pièce d'identité
  - La pièce d'identité du client, y compris le numéro de la pièce d'entité et toute autre information nécessaires conformément aux lois et règlements applicables
  - Adresse de domicile du client
  - Numéro de téléphone du client – Pour nous permettre d'empêcher le traitement des transactions illégales, si nécessaire.
  - Date de naissance du client – A renseigner dans le bon format comme l'exigent les systèmes de MoneyGram. Veillez à ne pas intervertir le jour et le mois.
- **D'autres informations peuvent être collectées le cas échéant :**
  - Numéro de compte bancaire du client
  - Numéro d'identification nationale ou d'identification fiscale,
  - Adresse e-mail du client
  - Profession du client (une description spécifique du poste et non une profession générique comme « manager » ou « indépendant »)
  - Lieu de naissance du client (correspond à ce qui est sur la pièce d'identité du client)
  - Référence de la transaction
  - Carte de crédit ou de débit
- **Aussi, les guichetiers doivent :**
  - Communiquer de manière claire à l'ensemble de la clientèle, la liste de tous les types de pièces d'identité acceptés par la loi comorienne en vigueur et fournie par la Direction Conformité de la SNPSF.
  - Les types de pièces d'identité acceptés sont :
    - ✓ Carte Nationale d'Identité (CNI)
    - ✓ Passeport
    - ✓ Récépissé de demande de CNI ou Passeport (accompagner de la CNI ou du Passeport)

Partie 3.2. Collecte de la pièce d'identité et vérification de l'identité des clients

- **N'acceptez qu'une pièce d'identité avec photo :**
  - Délivrée par un organisme gouvernemental comme un passeport ou un permis de conduire, une carte de résidence ou une pièce d'identité nationale
  - Non expirée
  - Pas modifiée ou fausse
  - Originale et non pas une copie
  - Acceptable selon les lois et règlements locaux.

- **La pièce d'identité doit fournir des détails sur :**
  - Prénoms et noms de famille
  - adresse
  - photographie
  - Signature/Tampon ou cachet
  - Date d'émission/expiration
  - Date et lieu de naissance

Ne pas traiter les transactions lorsque vous avez des doutes au sujet de l'identité du client!

- Vérifier la cohérence entre les informations sur la pièce d'identité, celles fournies par le client et le client qui présente les informations/pièce d'identité (le cas échéant) :
  - Le nom et la date de naissance renseignés par le client correspondent-ils au nom et à la date de naissance marqués sur la pièce d'identité qu'il a présentée ?
  - La pièce d'identité présentée correspond-elle à la personne debout devant eux (photo et informations correspondantes) ?
  - L'information sur la date de naissance fournie par le client correspond-elle à son apparence ?
  - La signature sur la pièce d'identité correspond-elle à la signature des clients sur le formulaire ou le reçu MoneyGram ?
  - Le tampon de l'autorité sur la pièce d'identité est-il cohérent avec le lieu d'émission ?

- **Vérifiez la pièce d'identité sous tous les angles:**
  - La pièce d'identité est-il surchargée ou avec des rayures ?
  - Lorsque vous passez votre pouce sur la pièce d'identité, il y a-t-il une partie qui est épaisse ou bosselée ou les bords sont-ils décollés?
  - La pièce d'identité est-il valide (date d'expiration) ?
  - Les informations d'identification saisies dans le système sont-elles correctes (éviter les erreurs de frappe)?

3.3. Protection des données personnelles des clients

- Pour protéger les informations concernant les clients contre l'accès, l'utilisation et la divulgation non autorisés, **les guichetiers doivent** :

- Demander et recueillir les informations personnels uniquement lorsque le système de transaction (ex. Western Union) l'exige. Le système définit les informations à saisir en fonction du montant de la transaction selon les exigences locales.
- Accéder et utiliser les informations personnels uniquement lors de la réalisation d'une transaction.
- Ne jamais créer ou saisir de fausses informations dans le système de transaction (ex. Western Union).
- Faire de leur mieux pour s'assurer que personne n'entende leur conversation, surtout lorsqu'ils demandent le nom, l'adresse, la date de naissance, le pays de naissance, la pièce d'identité du client, etc.
- Arrêter immédiatement le traitement de la transaction lorsque le client n'est pas en mesure ou ne veut pas donner l'information requise.
- Ne jamais montrer l'écran du poste de travail à un client.
- Eviter les erreurs de frappe afin d'assurer la satisfaction de la clientèle et le respect des exigences réglementaires.

- Assurer l'archivage et le stockage des reçus et des dossiers et assurer la destruction appropriée des documents après la période de conservation requise.
- Ne pas divulguer d'information à un tiers, y compris le conjoint ou un membre de la famille.
- Ne pas divulguer d'informations à un client sur son activité sans vérifier et authentifier l'identité du client.
- Ne pas divulguer d'information sur les clients sans demande formelle et écrite, comme une ordonnance du tribunal ou d'une autorité gouvernementale.
- Fournir des mesures de protection pour s'assurer que les renseignements personnels sont protégés afin d'empêcher l'accès et l'utilisation non autorisés. Cela s'applique aussi bien aux données physiques qu'électroniques.
- S'assurer d'avoir une connexion individuelle.
- Identifier et signaler les failles de sécurité.
- S'assurer d'avoir accès aux politiques et/ou aux procédures de la SNPSF relatives à l'utilisation personnelle des produits et services. Ces procédures sont également requises pour tous les employés de la SNPSF quelque soit leur poste de travail, particulièrement la Direction Générale.
- Ne pas initier, traiter ou compléter des transaction de type transfert/réception de fond pour leur propre compte ou pour le compte des membres de leur famille proche.

Lorsque les clients ont une question concernant la gestion de leurs données personnelles, invitez les à contacter le service Conformité !

Les exigences de la SNPSF en matière de Conformité

PARTIE 4 :
PRÉVENTION DE LA FRAUDE

4.1. Définition de la fraude

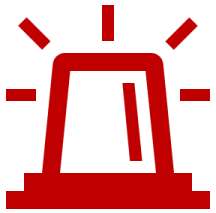
- **Qu'est-ce que la prévention de la fraude?**

  - **Prévenir la fraude et les escroqueries,** c'est-à-dire le vol d'informations et d'argent par tromperie, tricherie, manipulation ou tout autre moyen illégal de mettre les agents et/ou les clients en danger.

- **Quelles sont les deux principales catégories de fraude?**

  - **Fraude d'agent :** quand les agents risquent de perdre des fonds en exécutant des transactions qui sont frauduleuses. En tant qu'agents, vous êtes souvent la cible de personnes qui tentent de voler des renseignements ou qui tentent d'effectuer des transactions frauduleuses au profit du criminel ou du fraudeur.
    → Les tests des transactions, les imposteurs se faisant passer pour des autorités, la mise à jour de logiciels, la transaction téléphonique, le phishing (e-mails ou sms).

- **Fraude à la consommation :** lorsque le client est **victime de fraude**. Historiquement, les personnes âgées sont plus souvent la cible des fraudeurs.
  → Loterie ou concours, fraude aux achats en ligne / Internet, fraude à la personne dans le besoin / urgence, Fraude sentimentale, escroquerie aux impôts, escroquerie ou faux prêt/crédit, escroquerie à l'héritage, escroquerie à l'emploi, escroquerie de preuve de fonds pour la location d'un appartement.



4.2. Identification de la fraude ciblant les clients

- **En tant que guichetier de la SNPSF, il est important de comprendre comment :**

  - Détecter la fraude ciblant les clients;
  - Aider ou mener des enquêtes sur la fraude;
  - Prévenir, signaler et gérer les transactions suspectes.

- **Signes pour détecter la fraude :**

  - Il n'y a aucun lien familial apparent entre le donneur d'ordre et le bénéficiaire des fonds (noms de famille différents par exemple);
  - Il ne semble pas y avoir d'objet économique pour la transaction;
  - Le client envoie de l'argent à une personne qu'il n'a pas réellement rencontrée, pour payer ses déplacements;
  - Il y a tellement de donneurs d'ordre impliqués dans la transaction qu'il semble peu probable que le bénéficiaire sache le nombre exact de personnes qui lui ont transmis de l'argent;
  - Le client est nerveux et semble suivre les instructions de quelqu'un d'autre au téléphone;
  - Un bénéficiaire utilise différentes pièces d'identité;
  - Le client a trafiqué ou falsifié des pièces d'identité;
  - Un bénéficiaire qui reçoit plusieurs transactions de la part de nombreux donneurs d'ordre (à plusieurs endroits);
  - Un bénéficiaire qui envoie immédiatement l'argent reçu de plusieurs donneurs d'ordre/transactions à un tiers (dans un nouvel emplacement);
  - Une personne qui tente de récupérer une transaction dans un pays/lieu autre que celui où elle devait être envoyée;
  - Plusieurs personnes entrent dans le lieu, mais un seul d'entre eux réalise une transaction.

4.3. Prévention de la fraude ciblant les clients

- Pour prévenir la fraude ciblant les clients, **les guichetiers doivent :**
  - ✓ Connaître leurs clients;
  - ✓ Déterminer et confirmer **l'identité des clients;**
  - ✓ **Poser des questions** au client en cas de suspicion concernant la transaction, tels que :
    - Quel est le but de la transaction?
    - Comment connaissez-vous le donneur d'ordre? (ou bénéficiaire?) Avez-vous initié le contact avec le donneur d'ordre? (ou bénéficiaire?)
    - Êtes-vous sûr que la personne qui vous a contacté est vraiment dans le besoin?
    - A quand remonte la dernière fois que vous l'avez rencontré en personne ?
    - Dans quel secteur d'activité travaillez-vous?
    - Avez-vous croisé l'information avec un autre membre de votre famille avant d'envoyer de l'argent d'urgence à la personne qui vous a contacté?
    - Avez-vous joué à la loterie ou participé à un concours? Avez-vous acheté un billet ou avez-vous participé à un tirage au sort?
    - Êtes-vous sûr que la personne à qui vous envoyez de l'argent travaille réellement pour l'entreprise qu'elle prétend représenter? Avez-vous vérifié qu'il s'agit d'une entreprise connue/réputée?
  - ✓ S'assurer de bien connaitre les **escroqueries frauduleuses courantes** qui traitent des transactions.

Si vous avez des raisons de croire que le client est victime de fraude - NE PAS traiter la transaction

4.4. Prévention de la fraude ciblant les agents (1/2)

Pour prévenir la fraude ciblant les agents, les guichetiers doivent :

- S'assurer d'être suffisamment formés sur les directives concernant la prévention de la fraude et les techniques illicites de fraude.
- Raccrocher immédiatement si quelqu'un les appelle et leur demande de traiter une transaction, y compris si on leur demande de réaliser un « test » par téléphone.
- Supprimer ou restreindre les fonctions de renvoi automatique d'appels sur leur téléphone professionnelle.
- Protéger et changer le PIN/mot de passe régulièrement et à chaque départ.
- Ne pas ouvrir des pages Internet non sécurisées.
- Faire attention aux messages pop-up qui prétendent que la machine est infectée et proposent un logiciel pour scanner ou résoudre le problème.

4.4. Prévention de la fraude ciblant les agents (2/2)

Pour prévenir la fraude ciblant les agents, les guichetiers ne doivent PAS :

- Partager des informations confidentielles avec un tiers.
- Envoyer des transactions de « test », de « formation » ou de « fausses » transactions.
- Envoyer les transactions sans l'argent en main ET le client physiquement présent avec eux.
- Effectuer des transactions de toute nature par téléphone.
- Partager leur PIN/Mot de passe avec un tiers.
- Énoncer leur PIN/mot de passe devant un client ou l'afficher là où un tiers peut le voir.
- Partager leur PIN/Mot de passe par téléphone.
- Ouvrir les messages pop-us, y compris ceux qui prétendent que l'ordinateur est infecté ou qui offrent de scanner l'ordinateur.
- Répondre ou ouvrir des pièces jointes ou cliquer sur des liens dans des e-mails non sollicités sur n'importe quel ordinateur.
- Naviguer sur internet, utiliser la messagerie instantanée, ou utiliser les services bancaires en ligne sur les ordinateurs utilisés pour la réalisation des transactions.

Les exigences de la SNPSF en matière de Conformité

PARTIE 5 :
SURVEILLANCE DES TRANSACTIONS : DÉTECTION ET ESCALADE DES ACTIVITÉS SUSPECTES

5.1. Définition des activités suspectes

Qu'est-ce qu'une activité suspecte?

Toute transaction inhabituelle, hors du commun pour un client ou liée à la fraude.

Quelles sont les principales activités potentiellement suspectes à signaler?

- Transactions impliquant le financement du terrorisme ou le blanchiment d'argent, la fraude, les escroqueries, etc.
- Lorsque le donneur d'ordre ou le bénéficiaire ne peut pas être clairement identifié.
- Transactions complexes ou sans motif économique ou objet légitime ou avec un montant anormalement élevé ou pour lesquelles le doute ne peut être levé après une investigation plus approfondie.

Pourquoi est-il important d'identifier et de signaler les activités potentiellement suspectes?

- Cela est exigé par la loi et les règlements :
- Pour éviter les sanctions réglementaires.
- Pour protéger la réputation de l'entreprise.
- Pour protéger le travail de l'agent.
- Parce que c'est la bonne chose à faire !

Suivant la politique de la SNPSF, les guichetiers ne doivent pas :

- Traiter une transaction soupçonnée d'être liée à des activités illégales. Les produits et services de la SNPSF ne sont utilisés qu'à des fins légales.
- Participer sciemment à des activités liées à la fraude, au blanchiment d'argent, au financement du terrorisme ou à toute autre activité illégale ou les faciliter.

Une transaction peut paraître suspecte pour un client et ne pas paraître suspecte pour un autre. Les activités suspectes peuvent être observées « en temps réel » (informations obtenues en présentiel le cas échéant) en fonction de la formation des agents, de la connaissance des clients et de la vigilance de l'agent.

5.2. Détection des activités suspectes

Plusieurs facteurs peuvent vous aider à déterminer si la transaction d'un client est potentiellement suspecte dont :

Le montant de la transaction

Les réglementations et les lois comoriennes peuvent vous obliger à recueillir des informations auprès des clients à partir d'un certain montant.

Le pays où est localisée votre entreprise

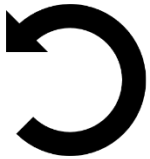
Les autorités et les régulateurs ont identifié des zones géographiques comme étant très à risque d'activités criminelles.

Transaction inhabituelle réalisée par un client « régulier »

Clients « réguliers » qui effectuent des transactions inhabituelles par rapport à celle réalisées précédemment.

Commentaire ou comportement suspect d'un client

Les commentaires ou comportements suspects et inhabituels d'un client.



Une tentative de transaction qui semble suspecte

Une transaction qui a été interrompue quelle que soit la raison et qui:

- N'est pas seulement une requête.
- Est potentiellement suspecte.
- Aurait été signalée aux régulateurs si la transaction avait été réalisée.

5.3. Exemples d'activités suspectes

- Un client qui envoie de l'argent à plusieurs bénéficiaires (dans différents pays) ou à un client qui reçoit plusieurs paiements le même jour de différents donneurs d'ordre.
- Plusieurs clients qui envoient de l'argent au même bénéficiaire.
- Un client effectue une ou plusieurs transactions d'un montant exceptionnellement important, selon l'historique, la fonction ou du niveau de revenu du client.
- Un client (souvent âgé) qui envoie de l'argent à une personne qu'il n'a pas réellement rencontrée, pour payer un voyage ou pour une affaire « trop belle pour être vraie »
- Un ou des client(s) changeant fréquemment ou fournissant des informations personnelles incohérentes (adresses ou documents d'identité multiples) ou de faux documents d'identité
- Plusieurs clients tentent d'utiliser le même pièce d'identité
- Un client utilise les mêmes adresses, numéros de téléphone ou pièces d'identité similaires à celles d'autres clients

- Un client (ou un groupe de clients travaillant ensemble) envoie ou reçoit des transferts d'argent en deçà des exigences légales.
- Un client refuse de procéder à une transaction lorsqu'on lui demande une pièce d'identité ou vous demande comment éviter de fournir des informations personnelles supplémentaires ou tente de vous soudoyer ou de vous forcer à effectuer une transaction sans recueillir les renseignements appropriés.
- Un client pose beaucoup de questions au sujet des exigences en matière d'identification ou semble excessivement nerveux, anxieux ou agressif à l'idée de fournir l'information.
- Une tentative de transaction, c'est-à-dire la transaction qui n'est pas réalisée quelle que soit la raison, même si le client a d'abord demandé d'envoyer ou de recueillir les fonds et a fourni son nom à l'agent (directement ou par le biais d'un formulaire).
- Transactions complexes ou sans motif économique
- Transactions pour lesquelles vous ne pouvez pas lever le doute

5.4. Processus d'escalade des activités suspectes

Comment les guichetiers doivent-ils gérer les activités suspectes identifiées?

Vous refusez de traiter la transaction suspecte. **Ne réalisez pas une transaction si vous détectez une activité potentiellement suspecte!**

Vous devez signaler la transaction à votre hiérarchie immédiatement. Si vous réalisez **un rapport interne pour signaler une activité suspecte**, vous devez **conserver une copie** du rapport et de tous les documents justificatifs **pendant au moins 5 ans** à partir de la date à laquelle vous avez réalisé le rapport ou selon les exigences réglementaires locales.

En cas de transaction impliquant **le financement du terrorisme**, vous devez le **signaler directement et immédiatement aux forces de l'ord**re.

Vous devez veiller à ne pas « alerter» un client lorsque l'activité suspecte dans laquelle il est impliqué a été signalée.

Les exigences de la SNPSF en matière de Conformité

PARTIE 6 :
EXIGENCES RÉGLEMENTAIRES EN MATIÈRE DE REPORTING

La SNPSF et l'ensemble de ses partenaires doivent :

Pour la SNPSF

- **Fournir aux guichetiers des politiques et des procédures écrites** concernant le reporting des activités potentiellement suspectes ou des transactions en devises d'un montant important, et pour s'acquitter de toute autre obligation de reporting réglementaire dans la juridiction comorienne. Ces politiques et procédures devraient inclure l'obligation de ne pas « alerter » un client lorsque des activités suspectes ont été signalées.
- **Documenter les résultats de la surveillance de la lutte contre le blanchiment d'argent et de la lutte contre la fraude**, y compris le rapport d'activité suspecte ainsi que les décisions de réaliser le rapport ou de ne pas réaliser le rapport de rapports d'activités suspectes.

Pour les guichetiers

- **Signaler les activités suspectes** (y compris les tentatives de transactions) comme l'exigent les lois et règlements en vigueur.
- **Conserver des copies de tout document transactionnel ou justificatif ou rapport et des originaux** (ou de l'équivalent) pendant **au moins cinq ans**, ou plus si requis par la loi locale, à partir de la date de création du rapport .
- **Lister et documenter tout rapport additionnel exigé par la réglementation locale** (en plus de la divulgation de rapports d'activités suspectes et de rapports de transactions aux montants importants).

6.2. Outils de reporting réglementaire

- **Tout guichetier de la SNPSF ou d'un partenaire sous-traitant affecté au traitement de transaction directe de fond, a l'obligation de signaler les activités suspectes à la direction des Risques et de la Conformité de la SNPSF ainsi qu'aux autorités compétentes, comme l'exigent les lois en vigueur :**

  - Les activités suspectes des clients **peuvent être signalées par téléphone, par mail et/ou par courrier physique.**

  - Au besoin, réalisez **un rapport concernant les activités suspectes SAR/STR (Suspicious Activity/Transaction Report).**

  - Les activités suspectes **liées au financement du terrorisme** qui constituent une menace immédiate **doivent être signalées au SRF, au FinCEN** et/ou à tout autres Financial Intelligence Units à l'échelle mondiale.

Les exigences de la SNPSF en matière de Conformité

PARTIE 7 :
DROITS ET RÉCLAMATIONS DES CLIENTS

7.1. Droits des clients

Les guichetiers doivent :

- Agir avec honnêteté, intégrité et éthique avec les clients et lors du traitement d'une transaction.
- Réduire au minimum le risque de préjudice pour les clients et prévenir les cas d'actes ou de pratiques injustes et trompeuses (« UDAAP »).
- Protéger les données et la vie privée des clients.
- Empêcher les activités liées à la fraude.
- Divulguer toutes les informations requises aux clients au sujet de leurs transactions, y compris les renseignements relatifs aux frais et fournir toutes les communications avant et après paiement.
- Fournir aux clients des copies des reçus de transaction et qu'ils signent sur la copie de l'agent du reçu.
- Éviter les erreurs de frappe, y compris en ce qui concerne la saisie des informations des clients lors du traitement d'une transaction.

En cas de réclamation des clients, les guichetiers doivent :

- Enregistrer la réclamation.
- Ne pas essayer pas de résoudre une réclamation d'un client sans se coordonner avec la direction de la SNPSF.
- Travailler avec les clients pour résoudre les erreurs de transaction et les réclamations.
- Respecter toute exigence réglementaire additionnelle.

Afin de préserver l'image de la SNPSF et d'assurer la satisfaction des clients, les réclamations doivent être traitées le plus rapidement possible.

7.2. Réclamation des clients

- **En ce qui concerne les réclamations des clients, la politique de la SNPSF est de :**
  - Évaluer les réclamations de façon juste, cohérente et rapide.
  - Etudier les réclamations avec efficacité, assiduité et impartialité.
  - Prendre rapidement des mesures correctives.
  - Le cas échéant, suivre strictement les règles réglementaires stipulées et respecter les délais de réponse.
  - Fournir une résolution rapide, un suivi de l'état d'avancement et une réponse finale directe au client.
  - Dispenser une formation au personnel et aux agents partenaires sur les procédures de traitement des réclamations.
  - Examiner et signaler périodiquement l'analyse des tendances des réclamations s à la direction de la SNPSF.

- **Comment la SNPSF doit gérer les réclamations du client ?**
  - Les clients ont le droit de réaliser une réclamation jusqu'à 180 jours après la date de la transaction.
  - La SNPSF doit enquêter et répondre au client dans les 90 jours suivant la réception de la réclamation.
  - Assurez-vous que la réclamation verbale ou écrite est consignée.

Les exigences de la SNPSF en matière de Conformité

PARTIE 8 :
EXIGENCES EN MATIÈRE D'ARCHIVAGE ET DE CONSERVATION DES DOCUMENTS

8.1. Exigences en matière d'archivage et de conservation des documents

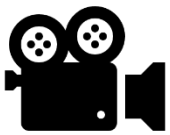
Pour satisfaire aux exigences en matière de conservation des documents, la SNPSF et ses partenaires doivent :

- Conserver tous les documents qui prouvent les efforts menés pour surveiller, prévenir et signaler la fraude, le blanchiment d'argent et le financement du terrorisme.
- Conserver les documents et fichiers (papiers, formulaires, reçus et autres documents confidentiels) dans un endroit sûr, sécurisé et verrouillé tel qu'un coffre fort ou une armoire sûre et verrouillée.
- Conserver les documents pendant au moins 10 ans ou plus, comme l'exige la réglementation comorienne.
- Déchiqueter/détruire tous les documents contenant des informations personnelles d'identité à la fin de la période de conservation légale, avec une déchiqueteuse, un service de déchiquetage professionnel ou tout autre façon de les rendre illisibles.
- Supprimer toutes les informations personnelles d'identité en fonction des exigences d'archivage des documents à la fin de la période de conservation légale.
- Stocker et sauvegarder tous les fichiers électroniques.
- Utiliser une politique de « bureau vide ».

8.2. Archivage et conservation des documents – Liste des documents

Les types de documents à conserver sont les suivants :

- Tous les reçus des transactions ;
- Les mises en œuvre des politiques et des procédures de conformité ;
- Les rapports effectués par le département conformité ;
- Les rapports de transactions inhabituelles/suspectes générés par l'outil de surveillance des transactions (ou les extractions à partir de l'outil ERP le cas échéant) ;
- Les analyses (y compris la décision finale) des transactions/activités identifiées dans le cadre de la surveillance AML /CFT des transactions et de la lutte contre la fraude ;
- Les rapports d'activités et de transactions suspectes (SAR et STR) soumis à l'organisme de réglementation comorienne (BCC) et aux CTR, selon les exigences la réglementation comorienne ;
- Les rapports exigés par l'organisme de réglementation pour les transactions supérieures à un seuil défini : reçus de transaction, pièce d'identité émise par le gouvernement ;
- Le contenu de la formation sur la conformité délivrée aux employés ou sous-agents.
- Les feuilles de présence aux séances de formation sur la conformité dispensées, pour identifier les personnes formées et qui ont obtenu la note requise et la date de la formation ;
- Les documents de formation des employés ;
- Les rapports des revues indépendantes effectuées, le cas échéant, avec les régulateurs comoriens ;
- Toutes les transactions traitées (nationales et internationales) par tous les clients (occasionnels ou non) ainsi que les informations connexes collectées (les raisons économiques...) ;
- Les réclamations des clients ;
- Les renseignements recueillis (ID, nom, date de naissance, etc.) auprès des clients pour toutes les transactions traitées et les documents de due diligence ;
- Les communications par courriel ou par voie postale.



Les exigences de la SNPSF en matière de Conformité

PARTIE 9 :
EXIGENCES EN MATIÈRE DE REVUE INDÉPENDANTE

9. Exigences en matière de revue indépendante

- La réglementation exige de la SNPSF qu'elle **se soumette à une revue indépendante périodique** et qu'elle se conforme à toutes les exigences légales comoriennes. Les revues indépendantes doivent être **documentées par écrit, conduites** par un **auditeur qualifié**, et non par le responsable conformité de la SNPSF et tenir compte de l'adéquation des éléments suivants dans le programme de la SNPSF :
  - Un programme écrit de lutte contre le blanchiment d'argent ;
  - l'autorité et l'expertise du Responsable conformité de la SNPSF ;
  - la formation des employés ;
  - la tenue des registres ;
  - les exigences en matière de surveillance et de reporting des transactions, y compris le reporting des activités suspectes ;
  - et/ou l'escalade des activités suspectes, le cas échant ;
  - le respect et la mise en œuvre de la Politique de conformité des partenaires.

- La SNPSF **doit documenter les mesures entreprises** en réponse à toute lacune associée aux produits et services identifiée lors de la revue indépendante.

Formation sur la répression des fraudes Visant les Clients des STA/ MTO

MOHAMED ELAMINE MZE
SNPSF
Responsable Risques et conformité de SNPSF

LA REPRESSION DES FRAUDES

LES SCENARIOS LES PLUS FRÉQUENTS DE FRAUDES DE L'ACTIVITE DES STA/MTO

INSTRUCTION

- Les scénarios suivants vous apprendront comment gérer certains éléments des situations fréquentes de transactions induites frauduleusement. Vous devrez déterminer la réponse appropriée de l'agent associé au comportement ou à la transaction du consommateur détails présentés dans ce scénario. Il y aura des cas où vous ne serez pas donné toutes les informations et devra utiliser ce que vous savez déjà pour faire un sélection. Assurez-vous de lire attentivement le scénario et tout contenu pertinent afin vous pouvez sélectionner le comportement correct.

- **SCEANRIO 1**

NOUVEAU CHIOT

Une femme veut envoyer un transfert d'argent pour 1 500,00 $ US. Elle semble heureuse et excitée et demande quand l'argent sera être disponible pour le récepteur.

SCEANRIO 1
NOUVEAU CHIOT

- CE QUE TU DEVRAIS FAIRE

POSER UNE QUESTION

Posez quelques questions pour mieux comprendre la transaction que vous effectuez. Vous répondez ses questions sur le fonctionnement des transferts d'argent, et alors vous lui demandez le but de son argent transfert. La dame dit qu'elle reçoit un chiot et doit envoyer d'abord l'argent pour que le chiot lui soit envoyé .

- DEMANDER UNE 2eme QUESTION

Vous demandez à la cliente si elle a rencontré le récepteur en personne. Elle vous dit non , mais qu'elle a été correspondant avec le récepteur qu'elle a contacté d'un site d'enchères en ligne.

- **CONSEILLER LE CONSOMMATEUR**

Vous refusez d'effectuer la transaction et de conseiller le consommateur de ne jamais envoyer de l'argent à quelqu'un qu'elle ne s'est pas rencontré en personne. Vous lui dites qu'elle pourrait être un victime d'une escroquerie d'achat Internet. Vous donnez aussi elle une brochure de fraude à la consommation et de souligner la types de fraude et de ressources pour plus d'informations.

SCEANRIO 1
NOUVEAU CHIOT

- **CE QUE VOUS NE DEVRIEZ PAS FAIRE**
- **EFFECTUEZ LA TRANSACTION**

Essayez de poser une question en premier. Rappelez-vous que c'est toujours un bonne pratique pour poser des questions au client pour obtenir une meilleure compréhension de la transaction.

- Vous ne devriez pas effectuer la transaction. Ce scénario ressemble à une **arnaque d'achat Internet**. Vous devriez donner au consommateur une fraude à la consommation brochure et souligner les types de fraude et ressources pour plus d'informations.

SCENARIOS 2 Aide à la famille

- **Un Client âgé qui semble contrarié et concerné veut envoyer 2 500,00 $ US**

- CE QUE VOUS DEVRIEZ FAIRE

POSER UNE QUESTION

Vous devriez toujours en savoir plus sur le transactions que vous effectuez, surtout quand une personne âgée ou un adulte à charge envoie argent. Quand vous demandez au consommateur ce qui ne va pas, il dit que son petit-fils lui a envoyé un e-mail en disant qu'il perdu son passeport et son portefeuille en voyageant à l'étranger et a besoin d'argent immédiatement.

POSER UNE SECONDE QUESTION

Vous demandez au consommateur s'il a essayé d'appeler son petit-fils ou quelqu'un d'autre pour confirmer si c'est un vrai d'urgence et le petit-fils est

- vraiment en difficulté. Le consommateur dit que son petit-fils lui a dit de ne pas le dire à quelqu'un parce qu'il a des ennuis et est embarrassé.

SCENARIOS 2 : AIDE À LA FAMILLE

- **CE QUE VOUS NE DEVRIEZ PAS FAIRE**

- EFFECTUEZ LA TRANSACTION

- Avant d'effectuer la transaction, vous devriez essayer pour obtenir plus d'informations sur le but de la transaction du consommateur.
- A tout moment une personne âgée personne ou un adulte à charge envoie de l'argent, vous devrait prendre le temps de trouver plus d'informations sur le but de leur transaction pour aider à déterminer s'ils sont une victime potentielle de fraude.

- Vous ne devriez pas effectuer cette transaction. Les agents de Western Union sont formés chaque année sur la façon d'aider à identifier et prévenir les aînés et les adultes dépendants d'envoyer de l'argent pour une arnaque, et cela ressemble exactement à l'escroquerie des grands-parents, ce qui est un type d'arnaque d'urgence. Vous devriez expliquer qu'il peut être une victime d'un grand-parent / **Scam d'urgence** et dire au consommateur qu'il devrait appeler son petit-fils ou un autre membre de la famille pour confirmer la situation d'urgence. Vous devriez aussi lui donner une brochure sur la fraude à la consommation et signalez-lui les types de fraude et les ressources pour plus d'informations.

SCÉNARIO 3
PREMIÈRE RENCONTRE

Une femme entre et doit envoyer 2 300 $ US.

Elle pose des questions sur le fonctionnement des transferts d'argent et à quelle vitesse le destinataire peut obtenir l'argent.

- CE QUE TU DEVRAIS FAIRE
- **POSER UNE QUESTION**

Vous devriez toujours poser des questions aux consommateurs sur leurs transactions, surtout si elles semblent être

- peut-être envoyer de l'argent pour la première fois.
- Vous demandez au client le but de son transfert. Elle dit qu'elle envoie de l'argent pour son petit ami pour lui rendre visite. Il habite dans un autre pays.

SCÉNARIO 3
PREMIÈRE RENCONTRE

- **POSER UNE SECONDE QUESTION**
- vous demandez au consommateur si elle l'a déjà rencontré ce petit ami en personne.

Elle dit depuis un an, et il vient vous dit encore qu'ils ont parlé en ligne enfin lui rendre visite

- Vous dites au client que vous ne pouvez pas effectuer la transaction car il semble qu'elle pourrait être une victime
- **d'une arnaque relationnelle**. Vous lui dites qu'elle devrait
- ne jamais envoyer d'argent à quelqu'un qu'elle n'a pas rencontré

la personne. Vous lui donnez une brochure sur la fraude à la consommation et souligner les types de fraude et les ressources pour Plus d'information.

SCÉNARIO 3
PREMIÈRE RENCONTRE

- CE QUE VOUS NE DEVRIEZ PAS FAIRE
- EFFECTUEZ LA TRANSACTION
- Ce consommateur pose beaucoup de questions sur le processus de transfert d'argent, comme elle pourrait envoyer un transfert d'argent pour la première fois

- Vous dites au consommateur que vous ne pouvez pas effectuer le transaction car il semble qu'elle pourrait être une victime d'une arnaque relationnelle. Vous lui dites qu'elle devrait ne jamais envoyer d'argent à quelqu'un qu'elle n'a pas rencontré la personne. Vous lui donnez une brochure sur la fraude à la consommation et souligner les types de fraude et les ressources pour plus d'information.

SCÉNARIO 4 : JOUR DE CHANCE

- Un homme s'approche. Il a l'air excité et heureux.
- Il veut envoyer 350,00 $ US
- **CE QUE VOUS DEVRIEZ FAIRE**
- POSER UNE QUESTION
- Vous demandez au consommateur comment il va et pourquoi il doit envoyer de l'argent. Il dit qu'il va bien. Il a gagné un tirage au sort, et il envoie de l'argent à couvrir les frais de traitement afin qu'il puisse réclamer son prix

POSER UNE SECONDE QUESTION

Vous demandez au consommateur ce qu'il a fait pour entrer dans la loterie

, et il dit qu'il n'a rien fait. Il juste eu une notification par e-mail pour réclamer ses gains

SCÉNARIO 4 : JOUR DE CHANCE

- **CONSEILLER LE CONSOMMATEUR**
- Vous dites au Client que vous ne pouvez pas effectuer le transaction parce qu'il semble qu'il pourrait être victime d'une arnaque de loterie / prix. Vous lui donnez un brochure de fraude à la consommation et souligner la fraude types et ressources pour plus d'informations.

- **CE QUE VOUS NE DEVRIEZ PAS FAIRE**
- EFFECTUEZ LA TRANSACTION
- Vous devriez toujours poser des questions sur la transaction.
- Vous ne devriez pas effectuer la transaction. Ce scénario ressemble à **une arnaque de loterie / prix possible.**

Vous devriez lui donner une brochure sur la fraude à la consommation et souligner les types de fraude et les ressources pour Plus d'information.

SCÉNARIO 5: RÈGLE DE VENTE DE TÉLÉMARKETING

- Un homme entre et doit envoyer US $ 25.00.
- CE QUE VOUS DEVRIEZ FAIRE
- POSER UNE QUESTION
- Vous devriez toujours essayer d'en savoir plus sur le transactions que vous effectuez même quand il est pour un montant faible.
- Vous demandez au consommateur le but de son transaction. Il dit qu'il envoie de l'argent pour un abonnement de magazine, il a acheté au téléphone hier soir.

- POSER UNE SECONDE QUESTION

Vous lui demandez s'il a reçu une vente de télémarketing appeler et si à travers cet appel, il a accepté d'acheter un abonnement au magazine. Il dit qu'il était d'accord acheter l'abonnement à un sport populaire magazine, et maintenant il fait le transfert de l'argent pour l'abonnement.

SCÉNARIO 5: RÈGLE DE VENTE DE TÉLÉMARKETING

CONSEILLER LE CONSOMMATEUR

Les consommateurs ne peuvent pas envoyer de transfert d'argent en utilisant

- Western Union en paiement de biens ou de services dans une réponse à un appel de vente par télémarketing. C'est
- illégal pour quiconque d'accepter les transferts d'argent de Consommateurs américains en paiement de biens ou de services offert ou vendu par télémarketing. Tu lui donnes une brochure sur la fraude à la consommation, soulignant la fraude
- types et ressources pour plus d'informations.

- C'est de L'arnaque de TELEMARKETING
- RÈGLE DE VENTE
-

SCÉNARIO 5: RÈGLE DE VENTE DE TÉLÉMARKETING

- CE QUE VOUS NE DEVRIEZ PAS FAIRE

- EFFECTUEZ LA TRANSACTION
- Vous devriez trouver plus d'informations sur le
- transactions que vous effectuez, même si c'est pour un petit montant

- Vous ne devriez pas continuer avec l'argent transfert si le consommateur envoie de l'argent comme paiement de biens ou de services en réponse à un appel de vente de télémarketing. C'est illégal pour n'importe qui accepter les transferts d'argent des consommateurs Comoriens comme paiement pour des biens ou des services offerts ou vendus par télémarketing. Vous lui donnez un consommateur brochure de fraude, en soulignant les types de fraude et ressources pour plus d'informations.
- CECI EST APPELÉ LE TELEMARKETING
- RÈGLE DE VENTE

SCÉNARIO 6 CONSOMMATEURS ENSEMBLE

- Trois hommes qui semblent être ensemble entrent dans votre magasin.
- Un seul s'approche, pour retirer l'argent qui lui était transféré . Les deux autres hommes se tiennent près de la porte

- **CE QUE VOUS DEVRIEZ FAIRE**

- **Vous devriez toujours poser des questions pour obtenir une meilleure** compréhension de la transaction, surtout quand
- **plusieurs personnes marchent et une seule personne est tentée d'effectuer de transactions**.
- Vous lui demandez quel est le but de sa transaction et sa relation avec l'expéditeur. Le consommateur regarde ses amis debout près de la porte. Il hausse les épaules et dit qu'il ne sait vraiment pas. Il dit que l'expéditeur est son ami, et il envoie juste de l'argent est gentil. Puis il change de ton et dit le l'expéditeur est son cousin, il a envoyé de l'argent pour qu'il puisse faire des réparations de voiture.

SCÉNARIO 6 CONSOMMATEURS ENSEMBLE

- **DEMANDER UNE SECOND QUESTION**
- Le consommateur semble confus, donc vous voulez obtenir plus d'informations pour voir s'il peut être impliqué dans un arnaque. Vous lui demandez s'il a reçu l'ordre de recevoir transaction par quelqu'un d'autre. Le consommateur a l'air Retour à ses amis à la porte à nouveau et hausse les épaules.
- Puis il dit non.

- CE QUE VOUS NE DEVRIEZ PAS FAIRE

- EFFECTUEZ LA TRANSACTION
- Essayez de poser une question en premier. Rappelez-vous que c'est toujours une bonne pratique pour poser des questions au consommateur pour obtenir une meilleure compréhension de la transaction, en particulier s'ils viennent avec plusieurs personnes

SCÉNARIO 6 CONSOMMATEURS ENSEMBLE

- Vous ne devriez pas effectuer la transaction. Ce scénario ressemble comme il peut être un paiement pour un arnaque. Vous devriez appeler la hotline de fraude quand le consommateur quitte l'emplacement, et alors vous devriez suivre vos consignes de signalement locales pour signaler situation à Western Union

- CE COMPORTEMENT EST APPELÉ
- CONSOMMATEURS CARTEL Travaille ENSEMBLE.
- **CONSEILLER LE CONSOMMATEUR**
- vous refusez d'effectuer la transaction et informez
- le consommateur que la transaction n'est pas disponible
- à présent. Vous appelez la hotline de fraude lorsque le consommateur
- quitte l'emplacement et vous suivez votre locale
- des directives pour signaler la situation à Western union.

SCENARIO 7: MULTIPLES TRANSACTIONS POUR UN

- Un consommateur vous remet trois formulaires de paiement qui sont pour les paiements provenant de différentes personnes dans différents pays, mais ils sont pour le même montant.
- CE QUE VOUS DEVEZ FAIRE

- **POSER UNE QUESTION**

Vous devriez être au courant des consommateurs qui reçoivent

plusieurs transactions de plusieurs pays. Demandez au consommateur le but de ses transactions.

Elle dit qu'elle retire de l'argent envoyé par les parents qui vivent dans ces pays. Quand elle montre son identité, son nom ne correspond à aucun des noms des expéditeurs et il semble y avoir pas relation familiale apparente.

SCENARIO 8 MULTIPLES TRANSACTIONS POUR UN

- CE QUE VOUS NE DEVRIEZ PAS FAIRE
- EFFECTUEZ LA TRANSACTION

  Vous devriez vraiment en savoir plus sur la transaction, notamment parce que le consommateur a retiré plusieurs transactions de plusieurs MTCN de différents endroits sans relation familiale apparente

- CONSEILLER LE CLIENT

- Vous dites au consommateur que la transaction n'est pas disponible dès maintenant. Vous appelez la hotline de fraude quand le consommateur quitte l'emplacement, puis vous suivez vos consignes de signalement locales pour signaler situation à Western Union

SCÉNARIO 8 ENTRAÎNEMENT

- Une femme vient chercher un transfert d'argent, et comme elle parle pour vous, elle continue de regarder son téléphone. Quand elle te parle, il semble qu'elle lit à partir de son téléphone.

CE QUE VOUS DEVEZ FAIRE

POSER UNE QUESTION

Vous devriez toujours en savoir plus sur les transactions que vous effectuez, surtout quand le consommateur semble suivre les instructions de quelqu'un sur un téléphone mobile. Vous lui demandez le but de sa transaction. Au lieu de répondre, elle tape sur son téléphone. Après environ 30 secondes, elle dit qu'elle retire de l'argent envoyé par sa mère.

SCÉNARIO 8 ENTRAÎNEMENT

- POSER UNE SECONDE QUESTION
- Il semble que le consommateur soit entraîné. Donc vous lui demandez si elle a reçu l'ordre de recevoir la transaction par quelqu'un d'autre, et elle a l'air confus. Elle dit elle ne sait pas, mais elle a besoin de l'argent

- **CE QUE VOUS NE DEVRIEZ PAS FAIRE**
- EFFECTUEZ LA TRANSACTION

Avant d'effectuer la transaction, vous devez essayer d'obtenir plus d'informations sur le but de la transaction du client. À tout moment le consommateur semble être entraîné, même si c'est par téléphone ou par SMS, vous devriez prendre temps de trouver plus d'informations sur le but pour leur transaction pour aider à déterminer si elles sont consommateur recevant une transaction frauduleuse.

SCÉNARIO 8 Entraînement

- CONSEILLER LE CONSOMMATEUR

- Vous dites au consommateur que la transaction est indisponible maintenant. Vous appelez la hotline de fraude lorsque le client quitte l'emplacement, puis suivez vos directives locales pour signaler la situation à Western union.

- CE COMPORTEMENT EST APPELÉ Être entraîné.

- . Vous ne devriez pas effectuer cette transaction. le consommateur est confus et ressemble à ce qu'elle est être coaché par quelqu'un d'autre pour recevoir le transaction. Vous devriez appeler la hotline de fraude lorsque le consommateur quitte l'emplacement, puis vous devriez suivre vos directives de déclaration locales signaler la situation à Western Union

SCÉNARIO 9

MAUVAISE IDENTIFICATION

- Un homme vient chercher un transfert d'argent, et quand il vous montre son identité, il a l'air fané et usé. C'est une couleur différente de les autres ID que vous avez vus de cet état ou pays.

NIN, Photo et Adresse

- CE QUE TU DEVRAIS FA
- POSER UNE QUESTION

Parce que l'identifiant du **Client** est différent et semble être porté, vous lui demandez une seconde forme d'identification. Il a l'air confus et n'a pas comprendre pourquoi il aurait besoin de vous montrer rien d'autre. Il dit qu'il n'a pas d'autre forme d'identité.

SCÉNARIO 9

MAUVAISE IDENTIFICATION

- CE QUE VOUS NE DEVRIEZ PAS FAIRE

- **EFFECTUEZ LA TRANSACTION**

  L'ID du consommateur semble différent et semble être porté. Vous devriez lui demander de vous montrer une seconde forme d'identification

- Conseillez le client
- Une identité valide non expiré émis par un Gouvernement qui ressemble au consommateur dans la localité est requis pour payer la transaction. Parce que l'ID semble modifié et vous soupçonnez que transaction est liée à la fraude, vous dites au consommateur vous ne pouvez pas effectuer la transaction à moins de pouvoir vous montrer une autre forme d'identification (comme un carte de bibliothèque ou facture de services publics - quelque chose un fraudeur aurait très probablement pas). Vous appelez la fraude hotline lorsque le consommateur quitte l'emplacement et suivez vos consignes de signalement locales pour signaler situation à Western Union.

SCÉNARIO 9 : MAUVAISE IDENTIFICATION

- **CE QUE VOUS NE DEVRIEZ PAS FAIRE**

- **EFFECTUEZ LA TRANSACTION**

  L'ID du consommateur semble différent et semble être porté. Vous devriez lui demander de vous montrer une seconde forme d'identification

- **Conseillez le client**

Une identité valide non expiré émis par un Gouvernement qui ressemble au consommateur dans la localité est requis pour payer la transaction. Parce que l'ID semble modifié et vous soupçonnez que transaction est liée à la fraude, vous dites au consommateur vous ne pouvez pas effectuer la transaction à moins de pouvoir vous montrer une autre forme d'identification (comme un carte de bibliothèque ou facture de services publics - quelque chose un fraudeur aurait très probablement pas). Vous appelez la fraude hotline lorsque le consommateur quitte l'emplacement et suivez vos consignes de signalement locales pour signaler situation à Western Union

SCÉNARIO 9 : MAUVAISE IDENTIFICATION

Vous êtes tenus d'obtenir auprès du consommateur

• Une forme d'identification actuelle qui est conforme à la loi N° 8 de juin 2012/AU

• Nationalité Comorienne - carte d'identité, passeport, - passeport avec visa d'entrée valide ou carte de réfugié du HCR

• Les opérateurs doivent s'assurer de l'identité:

Est authentique;

Qui contient la photo du client effectuant la transaction;

est valable;

Est émise par le gouvernement;

Contient le nom du client

Si l'une de ces conditions n'est pas confirmée, la transaction doit être refusée

SCÉNARIO 10 FLIPPING (RETOUR)

- Une femme vient chercher 1 232 $ US. Une fois qu'elle a reçu l'argent, elle procède à envoyer ce montant exact à une personne différente dans un autre pays.

- **CE QUE TU DEVRAIS FAIRE**
- **POSER UNE QUESTION**

Vous devriez toujours poser des questions aux consommateurs sur leurs transactions, surtout si elles sont en train de choisir de l'argent et immédiatement envoyer cet argent autre part. Vous demandez au consommateur dans le but de deux transactions. Elle semble mal à l'aise et ne établir un contact visuel avec vous. Elle vous dit qu'elle est juste recevoir de l'argent d'un ami et envoie de l'argent à un autre ami.

SCÉNARIO 10 FLIPPING (RETOUR)

- **POSER UNE SECONDE QUESTION**
- Vous demandez au client depuis combien de temps elle la connaît l' amis qu'elle envoie l'argent à et il le reçoit de qui. Elle n'a toujours pas de contact visuel avec toi, et elle hausse les épaules. Elle ne semble pas vouloir vous donner plus d'informations.
- . Vous dites au consommateur que la transaction n'est pas disponible à présent. Vous appelez la hotline de fraude lorsque le consommateur quitte l'emplacement et suivez vos rapports locaux des directives pour signaler la situation à Western Union.

SCÉNARIO 10 FLIPPING (RETOUR)

- AVISER LE CONSOMMATEUR

- Vous dites au consommateur que la transaction n'est pas disponible à présent. Vous appelez la hotline de fraude lorsque le consommateur quitte l'emplacement et suivez vos rapports locaux des directives pour signaler la situation à Western Union

- CE COMPORTEMENT EST A
- PPELÉ FLIPPINGCE QUE VOUS NE
- **DEVRIEZ PAS FAIRE**
- EFFECTUEZ LA TRANSACTION
- POURQUOI ?
- LA REPONSE:

Ce client essaie d'envoyer de l'argent immédiatement après avoir fait le retrait . Vous devriez essayer de demander une question pour obtenir plus d'informations

TOUTES NOS FÉLICITATIONS!

- Vous avez terminé avec succès la formation sur la répression des fraudes de Western Union Bien sûr pour les associés. Vous devriez maintenant pouvoir aider à protéger les clients en apprenant à détecter, prévenir, signaler et gérer les inductions frauduleuses transferts d'argent. En tant qu'associé agent fournissant des services Western Union, vous devez être conscient de ce qui suit:
- Types de fraude à la consommation ;
- **Questions à poser aux consommateurs** pour les aider à déterminer si leur transaction a été induite frauduleusement ;
- **Actions à entreprendre si vous** soupçonnez qu'un consommateur est une victime potentielle de fraude ou un consommateur est un auteur de fraude (fraudeur);
- **Indicateurs potentiels liés au comportement et aux transactions** qui aident à identifier les consommateurs qui envoient ou reçoivent des transactions induites frauduleusement **Si vous soupçonnez qu'un client est victime d'une fraude ou commet une fraude, refuser de traiter la transaction, même si le consommateur insiste sur le fait qu'il est envoyé dans un but légitime et de signaler la situation à la Western Union Fraude Hotline ou votre numéro de support d'agent dédié.**

Maintenant suis-je conforme?

https://www.youtube.com/watch?v=QhEjX_LO1ck

Merci de votre attention !

Nous espérons que cette formation sur la conformité a été informative et utile.

SAMEDI 1ER JUIN 2024

A L'HOTEL LE RITAJ