TENDANCES ET ANALYSE

DES RISQUES DE BLANCHIMENT DE CAPITAUX ET DE FINANCEMENT DU TERRORISME

EN 2016

TRACFIN Traitement du Renseignement et Action contre les Circuits FINanciers clandestins

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ACTION ET DES
COMPTES PUBLICS

SOMMAIRE

Tracfin effectue chaque année une évaluation des principaux risques de blanchiment de capitaux et de financement du terrorisme (BC/FT) pesant sur le territoire français. Cette démarche procède de la déclinaison, au niveau national, de la recommandation n°1 des standards du Groupe d'action financière (GAFI), qui spécifie que « les pays devraient identifier, évaluer et comprendre les risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont exposés ». Cette recommandation est appuyée au niveau européen par l'article 7 de la 4e directive anti-blanchiment[1], qui invite chaque État membre à prendre les mesures appropriées pour évaluer les risques BC/FT auxquels il est exposé.

Les rapports « Tendances et analyse des risques » de Tracfin sont d'abord destinés aux professionnels assujettis, afin de les guider dans leur propre analyse de risques. Ils servent également de support d'échange avec les administrations impliquées dans la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB/FT), et de vecteur d'information pour le grand public (étudiants, chercheurs, journalistes).

Le rapport « Tendances et analyse des risques 2016 » vient en prolongement du rapport précédent. L'édition 2015, sans prétendre à l'exhaustivité, tenait à présenter sous un angle pédagogique le panorama le plus large possible des problématiques de blanchiment, telles que Tracfin peut les observer sur le territoire français. Le rapport « Tendances et analyse des risques 2016 » est plus sélectif dans le choix des thèmes retenus, qu'il traite de manière plus approfondie.

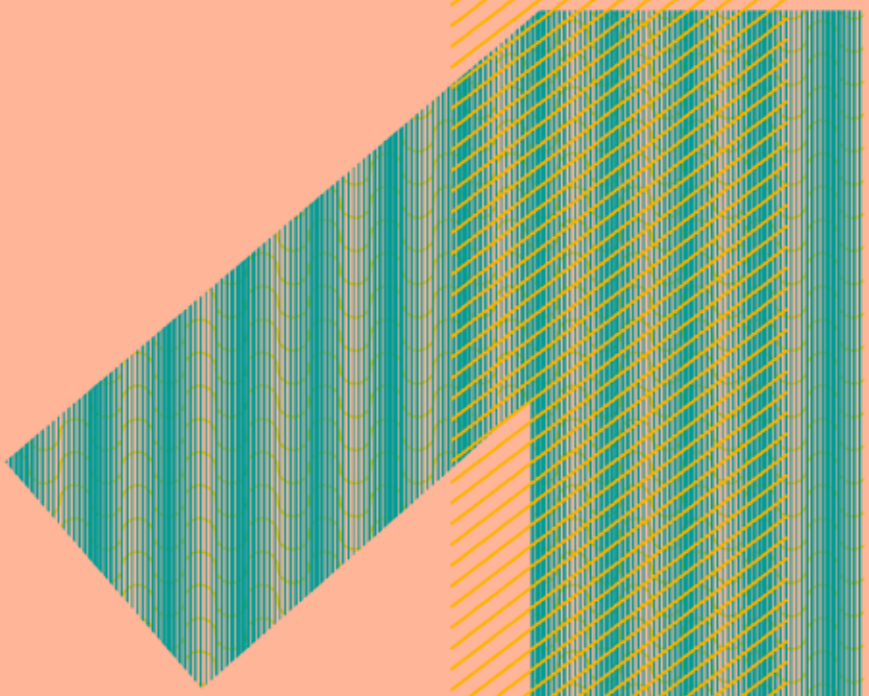
Tracfin alerte sur le niveau de la menace criminelle en matière financière : des schémas d'escroqueries d'ampleur continuent de se développer. Commis en bande organisée, ils sont dommageables pour l'économie.

Le rapport présente ensuite l'action de Tracfin dans la lutte contre le financement du terrorisme, qui reste une priorité essentielle du Service et l'objet principal des coopérations nationale et internationale.

Le rapport revient sur la lutte contre la corruption et la lutte contre les fraudes fiscales et sociales, qui constituent des missions de long terme de Tracfin. Elles suscitent une attente forte compte-tenu du contexte international, en particulier la mise en place de l'échange automatique d'informations fiscales.

Enfin, le rapport s'intéresse à la révolution technologique qui est en train de transformer le secteur financier, à commencer par les services de paiement et de transfert international de fonds. Ce bouleversement met au défi les banques commerciales installées, et par ricochet la règlementation LCB/FT, qui avait d'abord été conçue pour ce type d'acteurs.

1 (Directive UE n°2015/849)



EN MATIÈRE FINANCIÈRE, LES MENACES CRIMINELLES INNOVENT EN PERMANENCE PARALLÈLEMENT, LES MÉTHODES DE BLANCHIMENT CONVENTIONNELLES DEMEURENT

En matière financière, les menaces criminelles recouvrent deux types de phénomènes :

***A.** **Les escroqueries en bande organisée**, consistant à obtenir de la part des victimes, par des manœuvres frauduleuses, des remises de fonds indues. Leurs auteurs innovent sans cesse en exploitant systématiquement les failles de la réglementation sur les nouveaux produits et services financiers.*

***B.** **Les réseaux de blanchiment**, dont le but est d'évacuer les fonds d'origine délictueuse pour les recycler et les réintégrer dans l'économie légale. Les réseaux sont plus ou moins complexes et internationalisés en fonction de la nature et du volume des fonds à blanchir.*

Les réseaux d'escroquerie d'envergure, agissant en bande organisée, se conjuguent avec les réseaux de blanchiment internationaux à grande échelle. L'interaction est permanente.

LES RÉSEAUX SPÉCIALISÉS DANS LES ESCROQUERIES FINANCIÈRES DE GRANDE ENVERGURE CONTINUENT D'INNOVER

L'une des principales menaces criminelles identifiée par Tracfin est constituée de réseaux spécialisés dans des escroqueries sophistiquées à grande échelle. Ces réseaux se sont souvent constitués à partir d'escroqueries telles que les faux encarts publicitaires, les fraudes à la TVA (en particulier les carrousels), ou les faux rachats de créances au dépend des banques. Le rapport de Tracfin « Tendances et analyse des risques 2015 » montrait une diversification vers les escroqueries aux faux ordres de virement (FOVI) et les escroqueries aux sites de trading non régulés (options binaires, forex...).

Depuis 2016, Tracfin a constaté l'apparition de nouveaux champs d'opportunité pour les escrocs : les fraudes aux certificats d'économie d'énergie (CEE), les fraudes aux prélèvements SEPA, ou les propositions d'investissements en matières premières physiques, en particulier les diamants. Les réseaux d'escrocs identifiés peuvent aussi inciter d'autres agents économiques à la fraude, par exemple en proposant des services monétiques et des terminaux de paiement électroniques (TPE) leur permettant d'occulter une partie de leur chiffre d'affaires.

LES FRAUDES AUX CERTIFICATS D'ÉCONOMIE D'ENERGIE (CEE) : UN DISPOSITIF DÉTOURNÉ PAR LES ORGANISATIONS CRIMINELLES

Le fonctionnement du marché des CEE

Le dispositif des Certificats d'Economie d'Energie (CEE) a été mis en place en 2006 par les pouvoirs publics français[1]. Sa montée en puissance a été planifiée en plusieurs phases[2], tendant à une hausse rapide des volumes de CEE émis.

Le dispositif a pour but d'inviter certaines personnes morales à effectuer ou faire effectuer des travaux d'économies d'énergie. En échange, elles se voient remettre par les pouvoirs publics un nombre de CEE correspondant au volume d'énergie économisée grâce aux travaux effectués[3].

Le dispositif repose sur les **entreprises productrices d'énergie**, appelées les « **obligés** » (fournisseurs

1 Art. 14 à 17 de la loi n°2005-781 du 13 juillet 2005 de Programme fixant les Orientations de la Politique Energétique (dite loi POPE).

2 Phase 1 de 2006 à 2010 ; Phase 2 de 2011 à 2014 ; Phase 3 de janvier 2015 à fin 2017. Une quatrième phase est prévue à partir de 2018, devant donner lieu à un doublement des volumes.

3 Les économies d'énergie sont mesurées en « kWh cumac » (kilowatts heure cumulés actualisés). Ils correspondent aux kilowatts heure économisés grâce à l'installation d'appareils et d'équipements performants du point de vue énergétique.

d'électricité, de carburant, de fioul, de gaz de pétrole liquéfié, de gaz naturel, de chaleur ou de froid)[1].

Chaque producteur d'énergie obligé se voit assigner un objectif d'économie d'énergie, en fonction de ses volumes de vente. Pour remplir leurs objectifs, les obligés doivent détenir en fin de période un montant de CEE correspondant aux objectifs d'économie d'énergie qui leur avaient été assignés.

POUR REMPLIR LEURS OBJECTIFS DE CEE, LES OBLIGÉS ONT PLUSIEURS POSSIBILITÉS :

1/ Mener des actions d'économie d'énergie sur leur propre patrimoine, et les convertir en CEE auprès des pouvoirs publics.

2/ Faire mener des actions d'économie d'énergie à leurs clients, personnes morales ou ménages, en leur versant des aides.

L'obligé signe avec son client une « convention de financement de travaux en économie d'énergie ». Le client bénéficiaire transmettra une attestation de fins de travaux à l'obligé, que ce dernier pourra convertir en CEE auprès des pouvoirs publics. Le client bénéficiaire n'est jamais directement propriétaire de CEE et ne peut en faire commerce.

3/ Déléguer tout ou partie de leurs obligations à des sociétés tiers, appelées « délégataires », en signant avec eux un contrat ad hoc[2].

Il peut s'agir par exemple de sociétés du secteur du bâtiment ou des énergies renouvelables. Lorsqu'un délégataire signe un contrat en ce sens avec un obligé, il devient lui-même obligé. Il peut accéder au marché et recevoir des CEE des pouvoirs publics s'il justifie des travaux correspondants.

4/ Acheter des CEE de gré à gré auprès d'autres obligés, d'autres délégataires, ou d'une dernière catégorie d'acteurs appelés « éligibles ».

Les acteurs « éligibles » sont principalement les collectivités territoriales, les sociétés d'économie mixte et les bailleurs sociaux. Ils n'ont pas d'objectifs d'économies d'énergie à remplir, mais ils peuvent recevoir directement des CEE de la part des pouvoirs publics lorsqu'ils réalisent les travaux correspondants.

Les CEE sont comptabilisés dans un registre national tenu par une société privée, qui attribue à chaque acteur économique un compte individuel.

L'État ne définit pas les cours, ceux-ci s'ajustent sur un marché de gré à gré entre vendeurs et acheteurs.

Les travaux donnant droit à des CEE sont classés par secteur (agricole, industriel, tertiaire, transports, résidentiel). Ils correspondent à des opérations prédéfinies : 189 types d'opération ont été définis dans des fiches d'opération standardisées, précisant à chaque fois le volume forfaitaire d'économie d'énergie permis par chaque opération. Dans certains cas, ils consistent en des opérations spécifiques examinées en tant que telles par les pouvoirs publics.

Les CEE sont délivrés par le Pôle national des certificats d'économie d'énergie (PNCEE), qui vérifie l'éligibilité des opérations donnant lieu à la délivrance des CEE.

La non-atteinte de l'objectif par un obligé entraîne des sanctions pécuniaires. Les pénalités pour les fournisseurs d'énergie qui ne respectent pas leurs objectifs d'économies d'énergie consistent en des amendes représentant environ dix fois le montant des CEE manquants, au cours moyen de la période considérée.

Les failles du marché des CEE : la fraude documentaire

Les « délégataires » apparaissent comme les acteurs les plus sensibles du dispositif. Le coût d'entrée sur le marché des CEE pour un délégataire est faible car il nécessite seulement d'obtenir la délégation d'un obligé. Une fois que le délégataire a accès au marché, le risque est qu'il présente des dossiers fictifs, afin de bénéficier de CEE sans avoir effectué les travaux correspondants.

1 Art. L.221-1 et L.221-12 du code de l'énergie, ainsi que les art. R.221-1 et suivants.

2 Art. R.221-5 à R.221-7 du code de l'énergie

Le contrôle par le PNCEE de la réalité des travaux entrepris est rendu difficile par le peu de données transmises par les sociétés demandeuses, en particulier lorsqu'elles ont recours à de la sous-traitance. Aucun document justificatif n'est transmis a priori au PNCEE. L'obligé ou le délégataire ne doit présenter les documents détaillés qu'en cas de contrôles. De plus, le PNCEE ne dispose que d'une douzaine d'agents. Les contrôles, par échantillonnage et a posteriori, semblent insuffisants, même s'ils ont permis la détection de certaines fraudes. Début 2017, le PNCEE n'avait pas encore prononcé de sanctions.

Les bénéfices obtenus grâce à la fraude documentaire peuvent être maximisés par certaines dispositions du marché des CEE, qui incitent à l'opportunisme commercial.

La valorisation des CEE est calculée en fonction des performances énergétiques attendues sur le long terme par la réalisation de certaines actions d'économie d'énergie. Mais la valorisation ne tient pas compte du coût réel des travaux ou des matériaux installés. Certaines actions peuvent présenter facialement des performances énergétiques élevées, pour un coût réel minime. Parmi les 189 types d'intervention prédéfinis donnant droit à CEE, certaines sont plus rentables que d'autres. Les opérations les plus rentables font l'objet de campagnes de promotion massive auprès du grand public, par mailing ou spots radiotélévisés, de la part des sociétés fraudeuses.

De plus, la troisième phase du dispositif (2015-2017) a voulu soutenir les ménages en situation de précarité énergétique en obligeant les fournisseurs d'énergie à consacrer, en deux ans environ, un milliard d'euros d'aides aux travaux entrepris par les ménages aux revenus les plus faibles[1]. Les CEE « précarités » sont mieux valorisés que les CEE classiques, accentuant le risque de distorsion coût/bénéfice et donc l'incitation à l'arrivée d'acteurs mal intentionnés.

Tracfin traite un nombre croissant de dossiers de fraudes aux CEE.

Tracfin a observé une augmentation significative du nombre de dossiers en lien avec les fraudes aux CEE. Dans plusieurs cas, le Service a exercé son droit d'opposition afin d'éviter la fuite à l'étranger de capitaux frauduleusement acquis.

1 Cf loi du 17 août 2015 relative à la transition énergétique pour la croissance verte (LTECV).

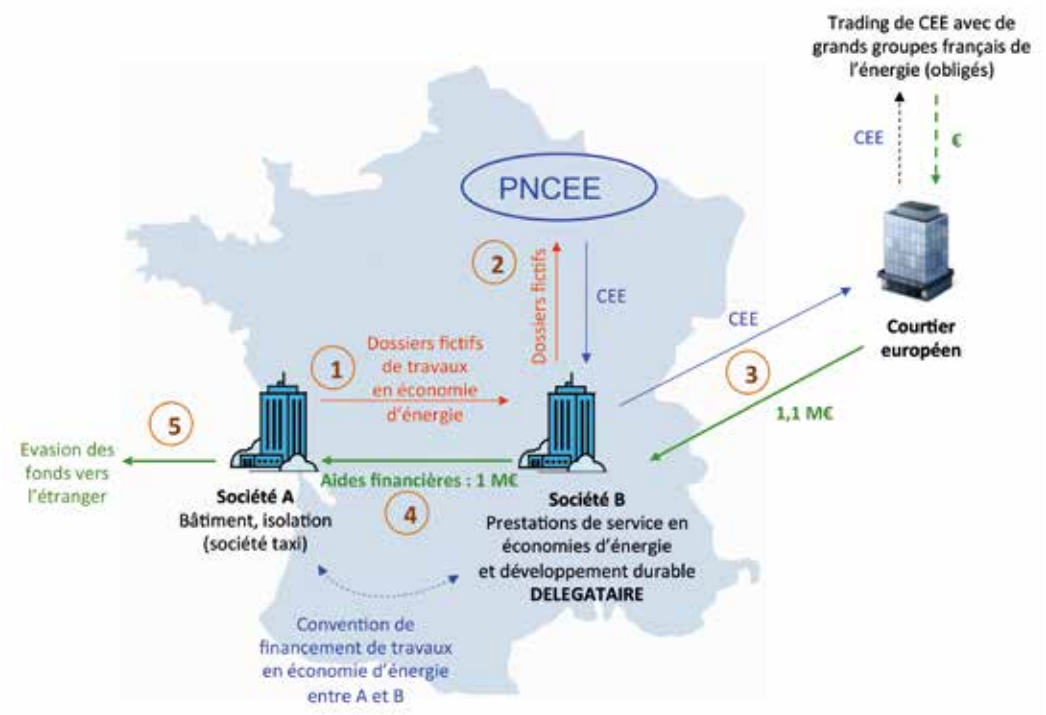
Cas n°1

L'attention de Tracfin est attirée par un déclarant sur l'activité de deux sociétés :

- La société A se présente comme une TPE du secteur du bâtiment, spécialisée dans les travaux d'isolation. Alors que son chiffre d'affaires annuel est de l'ordre de 350 k€ par an, elle reçoit en un trimestre pour près de 1 M€ d'aides financières de la part de la société B.
- La société B avait pour objet social le commerce d'articles de téléphonie mobile, et s'est récemment reconvertie dans les prestations de service aux économies d'énergie et au développement durable. Elle a obtenu le statut de délégataire auprès du PNCEE. Elle a effectivement versé en un trimestre près de 1 M€ d'aides financières à la société A, sous forme de chèques et de virements. Sur la même période, elle a vendu pour plus de 1,1 M€ de CEE à un courtier européen en produits d'énergie renouvelable.

Les sociétés A et B avaient signé une convention de financement de travaux en économies d'énergie, permettant à la société B de verser des aides à la société A pour l'inciter à mener ce type de travaux et à produire les justificatifs en conséquence. Les investigations de Tracfin ont permis d'établir que la société A avait produit de fausses attestations de travaux, utilisées par la société B auprès du PNCEE pour obtenir des CEE. Le total des CEE ainsi obtenus s'élevait in fine à 7 M€.

La société A était devenue le principal fournisseur de la société B. Elle n'avait pourtant ni le nombre de salariés ni les flux financiers pour justifier d'une activité suffisante dans le BTP nécessaire à la réalisation de tels montants de travaux. La structure de ses charges opérationnelles ne correspondait pas à celle d'une PME du secteur du BTP.



Cas n°2

La société G, délégataire, a encaissé des flux créditeurs de plus de 13 M€ en un peu plus d'un an, issus de la vente de CEE à d'autres délégataires. Un client principal, appelé société H, lui a acheté pour plus de 10 M€ de CEE. Sur les fonds ainsi récoltés, la société G a transféré à l'aide de fausses factures plus de 7 M€ à une société d'un pays d'Europe de l'Est, grossiste en meubles et en luminaires. Cette dernière a, dans un troisième temps, transféré les fonds perçus vers l'Asie. La société G paraît être l'unique client de la société d'Europe de l'Est.

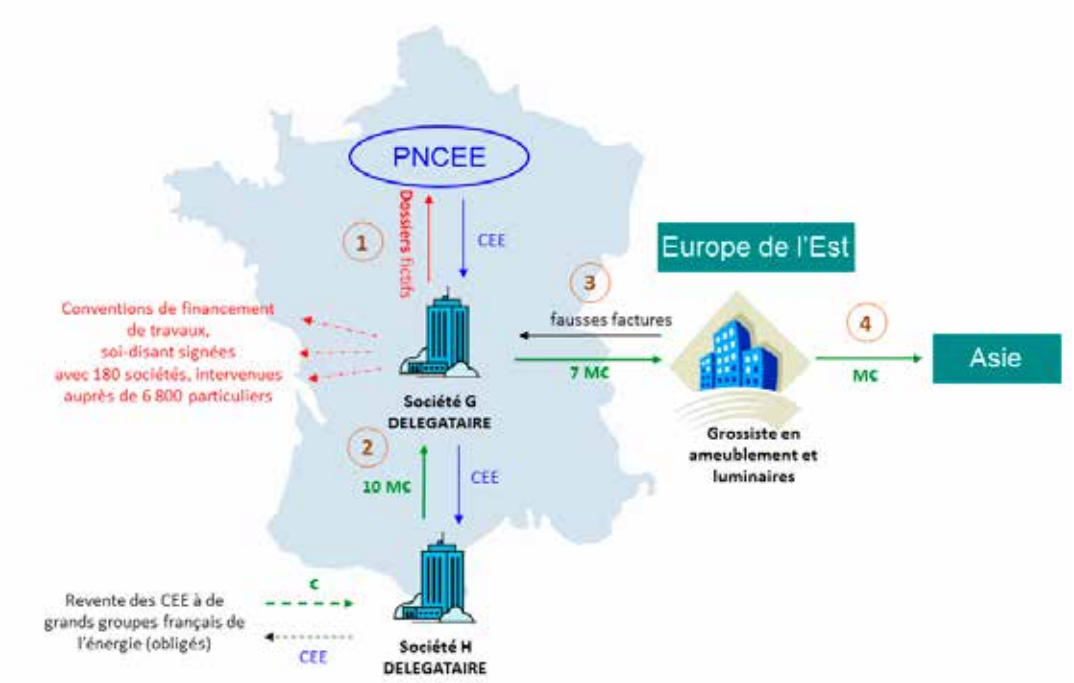
Les investigations menées par Tracfin ont mis en évidence une escroquerie aux CEE à l'aide de faux documents, dont le produit était blanchi par un circuit classique d'évasion de fonds bancaires frauduleux[1].

La société G avait justifié auprès du PNCEE la réalisation de 9 000 opérations auprès de 6 800 particuliers, par l'intermédiaire de 180 sociétés. La société G a expliqué signer des contrats avec des sociétés du bâtiment pour la valorisation d'économies d'énergie. La société G verserait une prime aux sociétés du bâtiment concernées pour chaque opération d'économie d'énergie réalisée, prime qui bénéficie au client final commanditaire des travaux. Puis, la société G reçoit les attestations de fin de travaux et les présente au PNCEE pour bénéficier des CEE correspondants. La société G a expliqué reverser 90% de la valeur des CEE aux sociétés du bâtiment partenaires.

Or, aucune des 180 sociétés de bâtiment n'a confirmé avoir réalisé les chantiers, ni touché de primes. La plupart des fonds étaient routés par la société G vers l'Europe de l'Est.

Le principal client de G, la société H, qui lui rachetait la plupart des CEE frauduleusement acquis auprès du PNCEE, les revendait à des obligés de taille importante.

Tracfin a exercé son droit d'opposition sur un flux de 2,2 M€ des comptes français de la société G vers un compte étranger. La Justice a pu ensuite saisir 5 M€.



1 Sur ces circuits d'évasion de fonds : Cf Rapport Tracfin « Tendances et analyse des risques BC/FT 2015 », p. 42 à 44 (cas n°15).

Ainsi, le dispositif des CEE s'apparente à **un mécanisme par lequel les grands groupes de l'énergie français sont amenés à financer des réseaux criminels transnationaux**.

Les énergéticiens doivent remplir leurs objectifs en achetant des quotas. Les réseaux criminels répondent à ce besoin, en générant des quotas sur la base de faux documents et de travaux fictifs. Le système est vicié car la nécessité du contrôle n'a pas été suffisamment prise en compte, ni dans son organisation ni dans son dimensionnement. Le statut de délégataire est obtenu facilement, sans avoir à produire de justifications suffisantes sur la nature de l'activité. L'Etat n'en subit pas directement les conséquences sur le plan financier, car il ne décaisse pas lui-même de fonds. Toutefois les objectifs de politique publique poursuivis à travers ce dispositif ne sont pas atteints.

La phase 4 du dispositif s'ouvrira en 2018. Elle prévoit une augmentation importante des volumes de CEE à produire par les obligés. Il existe un réel risque que les sociétés fraudeuses éludent les sociétés saines et que les CEE indus se substituent aux CEE légitimes.

Il est important de rappeler que **la liste des sociétés délégataires est publique**[1]. Les professionnels assujettis, en particulier les établissements financiers, doivent vérifier à partir de cette liste si leurs clients personnes morales sont des sociétés délégataires. Si c'est le cas, **Tracfin conseille de les placer en vigilance renforcée.**

1 Cf www.ecologique-solidaire.gouv.fr :

Choisir la rubrique : « Politiques publiques / Energies / Certificats économies d'énergie / Dispositif des Certificats d'économies d'énergie / Troisième période (2015-2017) ». Faire descendre la page.

Dans le sous-chapitre « Obligés de la P3 », une pièce jointe intitulée « Liste des délégataires au 2017-09-25 » est disponible en accès libre.

LES FRAUDES AUX PRÉLÈVEMENTS SEPA : LES EFFETS PERVERS DE L'HARMONISATION EUROPÉENNE ET DE LA LIBRE CIRCULATION DES CAPITAUX

Un autre type de fraude en cours de développement exploite les failles de la norme européenne SEPA (Single Euro Payments Area).

Définie par le règlement européen sur l'espace unique de paiement européen[2], la norme SEPA est pleinement entrée en vigueur le 1er août 2014. Elle a permis d'instaurer un espace homogène de paiement en euros, mettant fin à la mosaïque de standards et d'instruments nationaux qui prévalaient auparavant[3]. Elle a réorganisé les paiements bancaires au sein de la zone euro, en modifiant les processus de vérification à mener par les établissements bancaires avant de procéder à un paiement.

Le fonctionnement du prélèvement SEPA

La norme SEPA couvre trois instruments de paiement :

- Le virement (SEPA Credit Transfer ou SCT), qui impose aux banques une exécution en un jour ouvré maximum ;
- Le prélèvement (SEPA Direct Debit ou SDD) ;
- Le cadre d'interopérabilité pour les cartes SEPA (SEPA cards framework).

Le prélèvement SDD est l'instrument le plus vulnérable aux risques de fraude. Il consiste, pour un client, à autoriser une société à prélever sur son compte le montant des factures qu'il lui doit.

Le client donne une pré-autorisation (un mandat) à son créancier. C'est le **créancier** qui a la charge de dématérialiser et d'archiver le mandat signé par le débiteur, et de le présenter en cas de litige, et non plus la **banque du débiteur**. Il s'agit d'une innovation importante pour certains pays comme la France. Auparavant, c'est le banquier du débiteur qui avait en charge la gestion de l'autorisation, et était à même de vérifier que le mandataire avait bien un droit sur le compte bancaire dont il avait donné l'identifiant.

A présent, la banque du débiteur, lorsqu'elle reçoit une demande de prélèvement, présume l'existence d'un

2 Règlement n°260/2012 et règlement n°248/2014

3 Régis Boulaya (2013), *Les paiements à l'heure de l'Europe et de l'e-/m-paiement*, RB édition.

mandat et débite son client. A priori, ni la banque du débiteur ni celle du créancier n'ont l'obligation de vérifier l'existence du mandat.

Afin de protéger les usagers des prélèvements abusifs, les contestations ont été facilitées. La directive européenne sur les services de paiement (Directive 2007/64/CE du 13 novembre 2007, dite DSP1)[1], offre aux débiteurs des modalités de contestation et de remboursement du prélèvement SDD :

– pour les prélèvements autorisés : remboursement sur simple contestation dans un délai de **huit semaines** après l'émission du débit, quel que soit le motif.
– pour les prélèvements non autorisés : délai de 13 mois pour contester la mise en place d'un prélèvement (art. L.133-18 et L.133-24 du code monétaire et financier).
En cas de contestation du client débiteur, sa banque recrédite son compte. Puis elle se tourne vers la banque du créancier. Lorsque cette dernière reçoit l'instruction de remboursement, elle doit restituer les fonds à la banque du débiteur. Si elle ne peut se retourner contre son client, la banque du créancier assume le risque d'impayé sur ses fonds propres.

L'opposition comme la révocation d'un prélèvement portent sur le seul moyen de paiement et sont indépendantes de la créance sous-jacente. Il appartient au créancier de faire honorer la créance par son débiteur par tout autre moyen.

Un système perméable aux risques de fraude

Toute entité peut facilement effectuer un prélèvement sur un compte, et ce dans toute la zone SEPA. Elle devra simplement fournir à sa banque les données de comptes bancaires authentiques et les adresses de débiteurs, au format SEPA. Les fraudes s'appuient sur le caractère automatique du remboursement des prélèvements SEPA demandé dans les 8 semaines. Tracfin a constaté deux principaux schémas de fraude.

Le fraudeur perçoit des prélèvements non autorisés, mis en place à l'insu des débiteurs :

Avec le SDD, rien n'empêche une société fraudeuse d'ouvrir des comptes dans des pays peu regardants, d'obtenir des BIC et IBAN réels par des moyens légaux ou illégaux (*carding*), puis d'émettre une vague de prélèvements transfrontaliers, avant de virer les fonds vers des comptes tiers et de disparaître. Le fraudeur peut compter sur le manque de vigilance de certains débiteurs et sur les délais nécessaires pour faire remonter les contestations.

Les escrocs privilégient les prélèvements en fin de journée. Dans cette hypothèse, les vérifications ne pourront être réalisées par la banque que le lendemain matin, alors que les fonds seront crédités sur le compte bénéficiaire au cours de la nuit. Les malfaiteurs auront alors le temps de les transférer sur un compte tiers.

Le fraudeur émet des prélèvements autorisés puis demande leur remboursement :

Un fraudeur crée ou rachète une société et met en place, auprès de sa banque et de ses fournisseurs, une apparence de solvabilité en recevant des fonds conformément à son objet social. Il règle ses fournisseurs par prélèvements SEPA, en échange de prestations de services réellement effectuées. La société tend à augmenter ses achats de services à l'approche de la limite des 8 semaines permettant de contester les prélèvements.

Alors qu'elle a effectivement bénéficié des services en question durant les 8 semaines, la société demande le remboursement de l'intégralité des prélèvements effectués. Ce remboursement intervient automatiquement, et ses fournisseurs sont redébités par la banque du montant des prélèvements qu'ils avaient perçus. Les fonds recrédités sur le compte de la société fraudeuse sont immédiatement transférés vers un compte tiers à l'étranger. La société fraudeuse, vidée de toute substance, n'a plus aucun fonds disponibles lorsque le ou les fournisseurs se tournent vers elle pour obtenir le paiement de leur créance.

Ce type de fraude induit souvent des complicités entre certaines sociétés :

– Soit entre les sociétés débitrices et la société créancière, afin d'escroquer la banque de la société créancière. La société créancière sera défaillante, alors que les sociétés débitrices récupéreront leurs fonds tout en ayant bénéficié des prestations de services.
– Soit entre la société débitrice et ses clients, afin d'escroquer la société créancière ou la banque de celle-ci.

1 La DSP1 a été mise à jour par la DSP2 (Directive UE 2015/2366 du 25 novembre 2015), dont la transposition en droit français est intervenue au mois d'août 2017 (ordonnance n°2017-1252 du 9 août 2017).

Cas n°3 : escroquerie aux prélèvements SEPA

La société K est active dans l'achat/vente de matériels informatiques, de logiciels et de matériel bureautique. Mise en sommeil pendant trois ans, K a soudain changé d'actionnaire-gérant et réalisé en trois mois un chiffre d'affaires de 6 M€, en provenance de diverses sociétés de secteurs économiques variés perméables à la fraude (énergies renouvelables, sécurité, centres d'appel...).

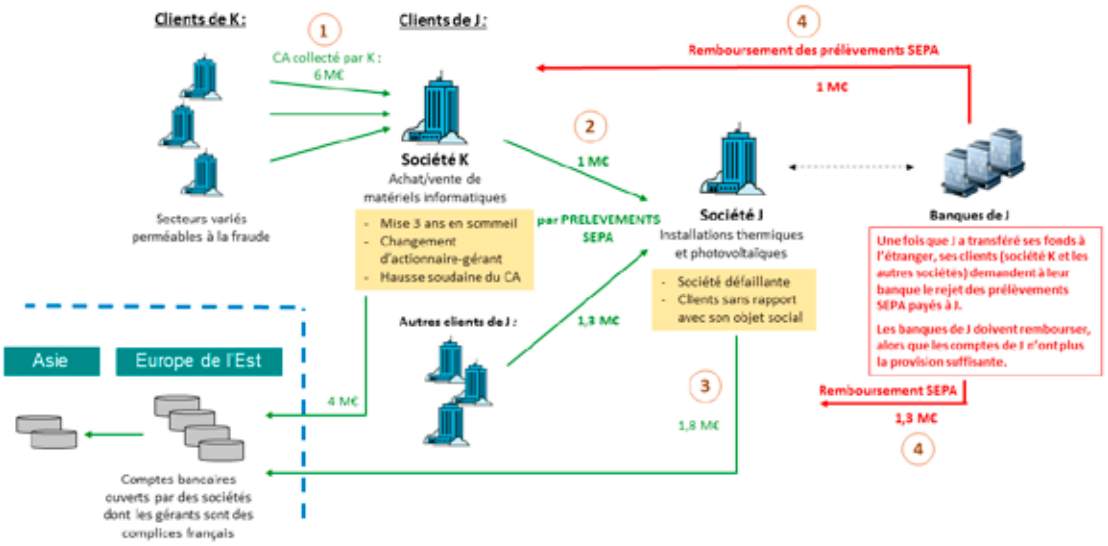
Le chiffre d'affaires collecté par la société K est reventilé ainsi :

- 4 M€ directement virés vers des comptes ouverts dans les pays de l'Est, par des sociétés dont les gérants sont français, puis re-transférés vers l'Asie ;
- 1 M€ vers une société J, sous forme de prélèvements SEPA.

La société J est active dans les travaux d'installations thermiques et photovoltaïques. Sa clientèle est constituée de nombreuses sociétés sans rapport avec son objet social, dont K. Elle se fait payer en grande partie par prélèvements SEPA.

La société J se trouve être une société défaillante. En cumulant les flux de K et d'autres de ses « clients » sans liens avec son objet social, elle a collecté par prélèvements SEPA un total de 2,3 M€ en trois mois. 1,8 M€ ont été renvoyés vers les sociétés des pays de l'Est.

Une fois les fonds transférés à l'étranger, K et les autres « clients » de J ont demandé le rejet des prélèvements SEPA. Les banques de J ont été obligées de re-créditer les comptes de K et des autres « clients », alors que les provisions des comptes de J n'étaient plus suffisantes.



Cas n°4 : dissimulation à l'étranger de CA non déclaré sous couverts d'achats payés par prélèvement SEPA

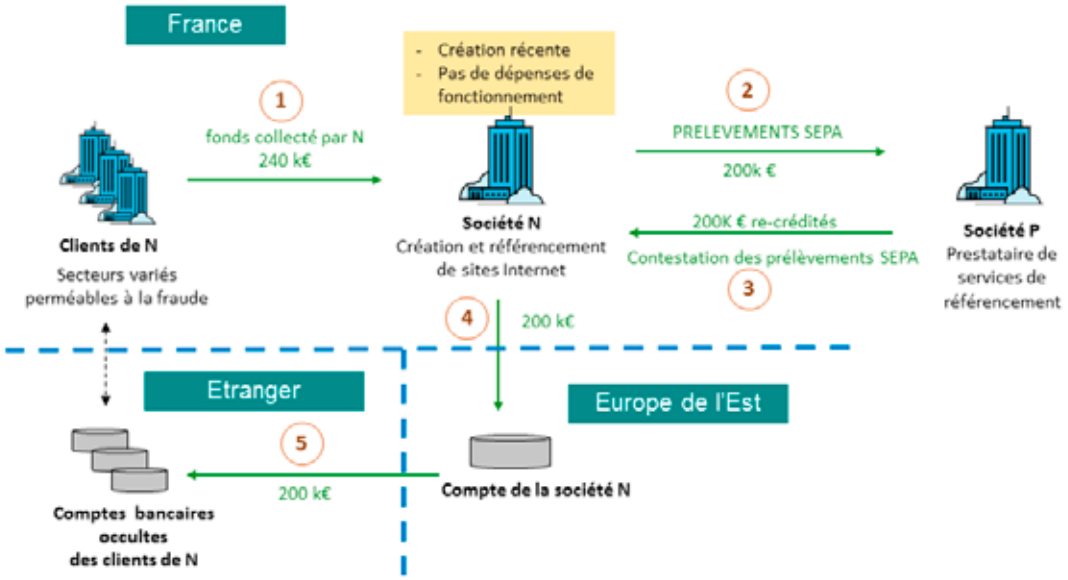
La société N, créée par un jeune gérant, propose des prestations de création de sites internet et de référencement de ces sites.

En 3 mois, N connaît d'emblée une forte activité en réalisant 240 k€ de chiffre d'affaires auprès de PME diverses (un commerce de décoration, un centre d'appel, deux sociétés de BTP...). Ces sociétés sont elles-mêmes de création récente, et défaillantes fiscalement et socialement.

Sur la même période, la société N ne présente aucun frais de fonctionnement : ni loyers, ni salaires. En revanche, elle affiche 200 k€ de flux débiteurs pour payer par prélèvements SEPA des services de référencement auprès d'un prestataire internet.

Moins d'un mois après les premiers prélèvements, le gérant de N conteste l'ensemble des prélèvements effectués. Conformément à la législation, il est intégralement re-crédité. Aussitôt, il transfère ces fonds à l'étranger, sur un compte ouvert dans un pays d'Europe de l'Est. Il peut alors les reverser à ses clients initiaux sur des comptes étrangers non déclarés.

L'opération aura permis aux clients de N de réduire leur résultat imposable en évacuant une partie de leur chiffre d'affaires à l'étranger, justifié comptablement par l'achat de prestations de référencement sur internet.



Cas n°5 : fraude au prélèvement SEPA et référencement internet

La société R est une société de création récente, spécialisée dans les dépannages à domicile (serrurerie, plomberie, travaux de rénovation et d'isolation...), principalement auprès des particuliers. En six mois, elle réalise plus de 400 k€ de chiffre d'affaires, dont 300 k€ perçus sous forme de chèques émis par des personnes physiques.

Cette performance commerciale n'est due qu'à une excellente visibilité sur internet, qui permet à la société R d'atteindre une large clientèle en un laps de temps très court. Les dépenses de la société sont constituées à 70% de frais de référencement auprès de prestataires internet, payés par prélèvements SEPA.

La société R fait rapidement l'objet de plaintes de clients dénonçant ses pratiques commerciales proches de l'escroquerie (surfacturation de dépannages d'urgence ou de prestations réalisées chez des personnes vulnérables...). Face à la montée des chèques contestés ou impayés, la banque de R clôt la relation.

Suite à cette décision, le gérant de R conteste l'ensemble des prélèvements qu'il a versés à ses prestataires internet pour son référencement. Ainsi, il a bénéficié des services de référencement, réalisé un chiffre d'affaires important, et s'est vu remboursé de ses frais de référencement.

LES ESCROQUERIES À L'INVESTISSEMENT EN MATIÈRES PREMIÈRES, DONT LES DIAMANTS PHYSIQUES

Depuis 2016, Tracfin constate une multiplication des offres douteuses de placements en diamants d'investissement. Le Service a traité de nombreux dossiers présentant des caractéristiques similaires. L'Autorité des Marchés Financiers (AMF) a publié plusieurs mises en garde sur ce type d'offres[1].

Les offres de placement en diamants d'investissements

Des sociétés d'investissement ou de courtage en pierres précieuses proposent sur internet d'investir dans des diamants physiques, présentés comme une valeur refuge permettant des rendements élevés. Ces sociétés utilisent la publicité sur internet, les spots radio ou télévisés, ainsi qu'un démarchage commercial agressif envers les particuliers.

Les diamants sont censés être conservés par la société dans des coffres au sein de ports francs, hors du territoire français. Le recours aux ports francs permet aux acheteurs d'être exonérés de TVA, selon le régime des entrepôts douaniers, ce qui accroît encore le rendement de l'investissement à la revente.

Ces modalités d'achat proposées aux particuliers sont de nature à faire douter de la réalité des diamants vendus. Les clients ne disposent pas de la marchandise achetée et ne semblent détenir aucun justificatif de propriété. Lorsqu'un client souhaite s'assurer de la réalité physique de son investissement, les relations avec la société se tendent. Les remboursements sont difficiles à obtenir, voire impossibles. La société peut vite devenir injoignable.

Même dans le cas où la société détient un certain stock de diamants, la valorisation des pierres est un processus complexe difficilement appréhendable par les non-initiés. A la différence des métaux précieux comme l'or ou l'argent, il n'existe pas de cours mondial public du diamant. Le marché du diamant est un système autorégulé qui fixe ses propres prix. Un indice y fait autorité : l'indice des prix Rapaport (Rapaport Price List), publié chaque semaine. Mais il est composite et établit des listes de prix par sous-catégories de diamants, en fonction de nombreux critères : poids de la pierre, qualité, stocks réels, production... Les sociétés d'investissement actives en France peuvent aisément présenter à leurs clients des valorisations faussées.

Dans ce type d'escroquerie, Tracfin a exercé à plusieurs reprises son droit d'opposition, afin de bloquer le transfert à l'étranger des fonds collectés auprès des particuliers. Certains bénéficiaires identifiés étaient déjà connus de Tracfin pour leur implication dans les escroqueries aux sites non régulés de trading de change (forex) ou d'options binaires.

1 Cf communiqués de presse de l'AMF en date du 6 janvier 2017, du 3 avril 2017 et du 24 juillet 2017.

Cas n°6 : escroquerie aux investissements en diamants

La société X, spécialisée dans le négoce et le courtage de diamants et pierres précieuses, a perçu un montant global de 8,8 millions d'euros dès ses dix premiers mois d'existence. Les flux créditeurs perçus sont majoritairement constitués de virements et chèques émis par des particuliers localisés sur l'ensemble du territoire français. Les comptes de la société enregistrent, au titre de la même période, des flux débiteurs d'un montant total de 8,6 millions d'euros dont plus de 6 millions d'euros émis à destination de l'étranger.

La société X propose à ses clients d'acheter des diamants qui seront placés dans des coffres sous sa responsabilité. Les acheteurs bénéficient, en contrepartie, de « l'exonération » de TVA sur leurs achats. Le diamant d'investissement est présenté par la société, sur son site internet, comme un placement d'avenir qui présenterait un rendement annuel supérieur à 6 %.

Les investigations effectuées par Tracfin ont permis de mettre en évidence un faisceau d'indices de nature à faire douter de la réalité de l'activité de la société X.

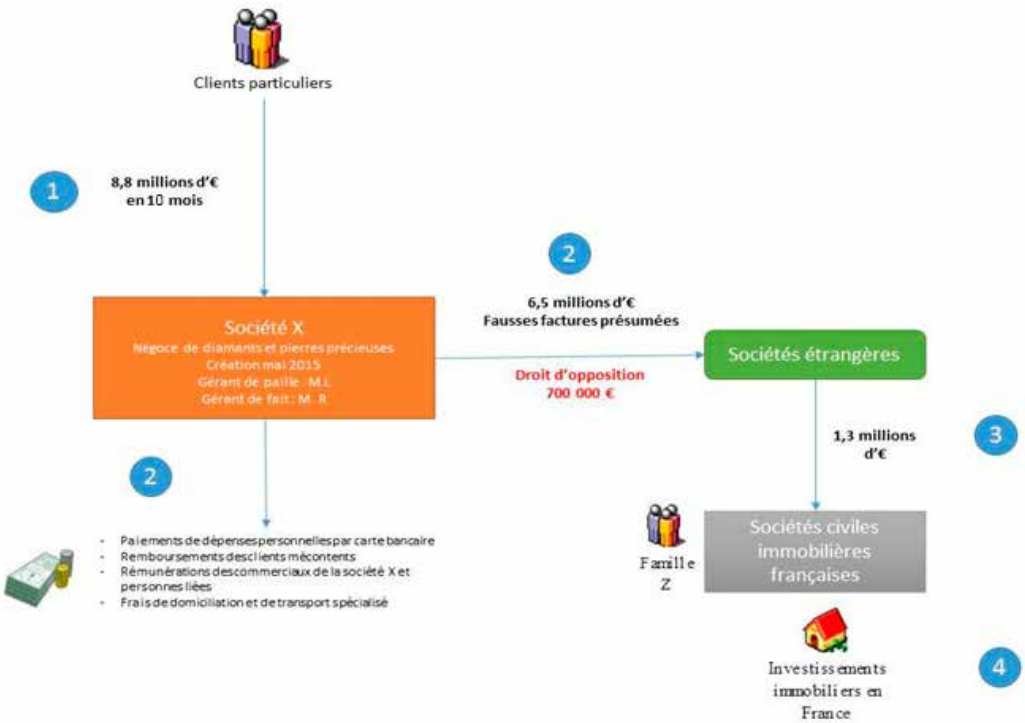
Les structures bénéficiaires de fonds à l'étranger sont apparues difficilement identifiables, ou leur activité sans lien avec l'activité économique de la société X. Des incohérences entre les déclarations fiscales et douanières déposées par la société et les flux bancaires enregistrés sur ses comptes laissent supposer la production de fausses factures auprès des établissements bancaires. Le recours systématique à des adresses de domiciliation par la société X est de nature à renforcer les doutes quant à la réalité de son activité.

Au débit, ont été relevées des dépenses de rémunération de commerciaux, des remboursements de clients mécontents et d'importants flux vers l'étranger. L'analyse des informations collectées auprès de nos homologues étrangers a permis d'identifier le circuit de blanchiment en France d'une partie des fonds émis par la société X à destination de l'étranger (montant identifié de 1,3 millions d'euros) par l'intermédiaire de sociétés civiles immobilières procédant à des investissements immobiliers au bénéfice d'une famille dont les membres n'avaient aucune source de revenus déclarée.

Dans le cadre de son enquête, le service a exercé, à deux reprises, son droit d'opposition, sur plusieurs opérations de virements à destination de l'étranger dont le montant total s'élevait à 700 000 €. L'identification rapide des victimes potentielles et des sociétés présumées liées au réseau de l'escroquerie identifiée a permis, en collaboration avec les autorités judiciaires, d'opérer la saisie, à titre conservatoire, d'environ 2 millions d'euros sur les comptes français des auteurs présumés.

Critères d'alerte :

- société de création récente ;
- activité de placement à risque, qui fait l'objet d'avertissement de la part d'autorité de contrôle ;
- siège social situé dans une société de domiciliation ;
- changement de gérance ;
- flux créditeurs enregistrés très important sur une période de courte durée ;
- flux débiteurs à destination de l'étranger.



Les propositions d'investissements dans les terres rares

Le schéma d'escroquerie mis en place sur le diamant peut être dupliqué à d'autres types de matières premières. Les terres rares offrent l'avantage d'être un marché peu régulé et particulièrement volatil. Les minerais ou les métaux rares ne faisant pas partie des instruments financiers, les sociétés de négoce dans ce secteur n'ont pas à être agréées comme entreprises d'investissement. Les informations relatives à ces marchés sont parcellaires et peu accessibles aux particuliers.

Cas n°7

La société Z se présente comme un courtier en terres rares et en métaux stratégiques, en direction des industriels et des particuliers avertis. Selon les mêmes méthodes que les sociétés de placements en diamants, la société Z propose aux particuliers d'investir dans ces matières premières, qui seront stockées en zone franche à l'étranger, en franchise de droits de douane et de TVA. La société Z recourt à une adresse de domiciliation.

Les investigations menées par Tracfin ont permis d'établir qu'en quatre mois, la société Z avait enregistré en France des versements de particuliers pour 360 K€. Au débit, les dépenses de la société ne correspondent pas à des achats de marchandises. Le Service n'a pas trouvé trace d'achats de minerais correspondant aux versements des particuliers. Aucune déclaration en douane relative à des importations de minerais ni de terres rares n'a été déposée par la société Z.

Les flux débiteurs sont dirigés vers une société partenaire en charge des démarches commerciales, rémunérée 80 k€, et vers plusieurs personnes physiques pour environ 200 k€. Le dirigeant de la société Z semble être le principal bénéficiaire puisqu'il reçoit sur ses comptes personnels, dans un autre pays de l'Union Européenne, près de 100 k€.

Ces différents éléments semblent de nature à remettre en cause la réalité de l'activité de la société Z et constituent un possible délit d'escroquerie en bande organisée.

LES FRAUDES AUX TERMINAUX DE PAIEMENT ELECTRONIQUES (TPE)

Les réseaux spécialisés dans les escroqueries financières de grande envergure peuvent aussi inciter d'autres agents économiques à la fraude. Certains prestataires de services monétiques et de paiement, vraisemblablement contrôlés par des réseaux criminels, proposent à leurs clients des solutions pour mener des opérations de fraude fiscale et de blanchiment de fraudes diverses. En particulier, certains prestataires proposent à une clientèle de professionnels et de commerçants des terminaux de paiement électroniques (TPE) permettant de faire dériver une partie de leur chiffre d'affaires vers des comptes étrangers non déclarés.

Cas n°8

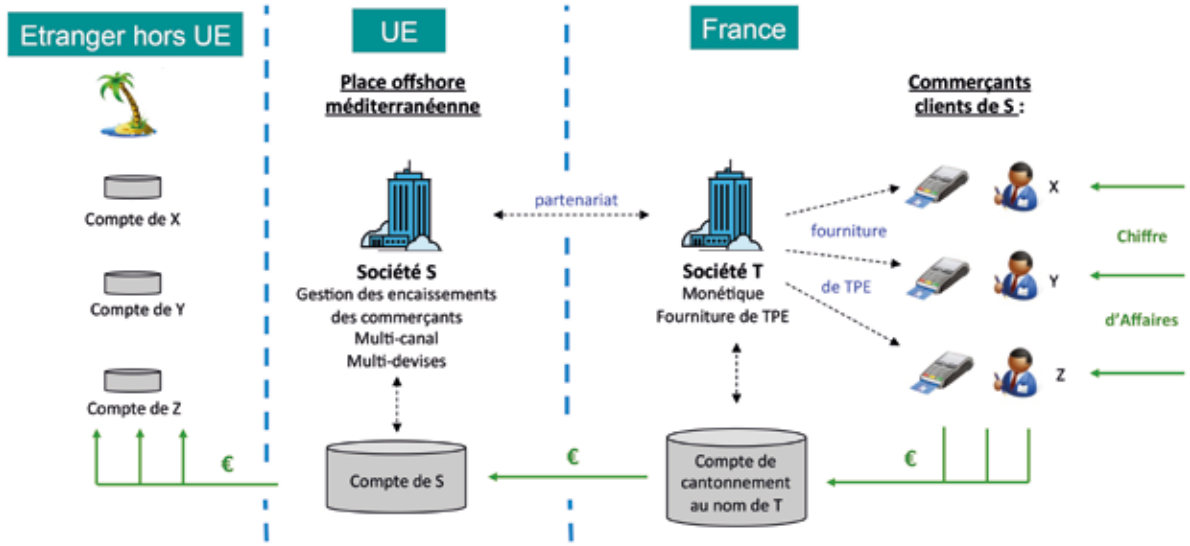
Une société S est établie dans une place offshore méditerranéenne. Elle propose aux professionnels et aux commerçants une gestion centralisée de leurs encaissements, quel que soit le canal de vente utilisé (physique, web, téléphone mobile), et dans un grand nombre de devises. La société S est agréée dans son pays comme établissement de paiement et intervient dans l'ensemble de l'Union Européenne sous le régime de la Libre Prestation de Services.

En France, elle travaille avec une société partenaire dénommée T, spécialisée dans les paiements électroniques et les services de monétique. L'activité paiements de la société T est agréée en France en tant qu'Etablissement de Paiement. Les sociétés T et S ont signé un contrat de prestation de services afin que la société T fournisse des TPE aux clients de la société S.

Les transactions effectuées sur les TPE de la société T sont centralisées sur un compte de cantonnement français ouvert au nom de T, ce qui permet de couper la trace des noms des commerçants bénéficiaires des transactions. Puis les fonds sont transférés sur un compte de la société S ouvert dans le pays où cette société est agréée. La société S reventile ensuite les fonds vers des comptes ouverts à l'étranger pour chaque client commerçant. Chaque compte est doté d'une carte bancaire étrangère utilisable par le commerçant pour son propre train de vie.

A nouveau, différentes méthodes de fraude et de blanchiment se superposent et s'interconnectent. Parmi les clients de la société S, Tracfin a identifié plusieurs sociétés impliquées dans des réseaux d'évasion de fonds bancarisés. Elles ont le profil de sociétés éphémères : sous-déclaration des recettes ; défaillance déclarative ; contrôles fiscaux en cours ; cessation d'activité ou clôture de l'activité commerciale alors que les comptes bancaires sont toujours actifs ; crédits bancaires sans lien avec l'activité ; virements importants à l'étranger...

Les sociétés S et T se rendent complices des fraudes commises par leurs clients professionnels et commerçants, et commettent les infractions de recel et de blanchiment du produit de ces fraudes.



Ainsi, la menace criminelle que constituent les escroqueries sophistiquées de grande ampleur repose sur des réseaux :

– très organisés dans leurs méthodes : ils recherchent systématiquement les failles des nouveaux dispositifs législatifs et réglementaires afin d'innover ;
– étendus et mouvants dans leur structure : un même réseau peut cumuler plusieurs activités. Les réseaux se superposent et s'entrelacent entre eux, ce qui crée des synergies entre les différentes escroqueries, les fraudes douanières, la fraude fiscale et le blanchiment.
Ces réseaux peuvent être en partie animés par des organisations criminelles transnationales.

L'opacité, l'étendue et l'agilité de ces réseaux les rend difficiles à contrer rapidement pour les autorités répressives. Ils mobilisent d'importants moyens d'enquête et aboutissent à des dossiers judiciaires complexes, dont le périmètre est parfois difficile à délimiter.

LE BLANCHIMENT CRIMINEL CONTINUE DE RECOURIR À DES MÉTHODES CONVENTIONNELLES

Parallèlement aux réseaux d'escroquerie en bande organisée, les autres menaces criminelles restent dépendantes des vecteurs classiques de blanchiment. Tracfin traite chaque année des cas issus du trafic de stupéfiants ou de l'immigration clandestine.

Les réseaux de moyenne envergure continuent de recourir massivement aux espèces : ils utilisent les services de transferts de fonds (sociétés de transmission de fonds) et les secteurs manipulant de grandes quantités d'espèces, tel que le secteur des jeux.

LES TRAFIQUANTS DE STUPÉFIANTS ONT RECOURS AUX ESPÈCES ET À LA FRAUDE COMPTABLE

Le recours aux services de transferts de fonds en espèces

En aval de la chaîne logistique du trafic de stupéfiants, les réseaux de distribution manipulent de grandes quantités d'espèces. Pour évacuer leurs gains vers l'étranger, ils recourent aux sociétés de transmission de fonds, qui proposent des services de transferts d'espèces à l'international. Les sociétés de transmission de fonds font preuve, pour la plupart d'entre elles, d'une vigilance accrue, grâce à des outils d'analyse des transactions qui détectent des incohérences soit de la part des expéditeurs, soit de la part des bénéficiaires.

Dans le cas des expéditeurs :

Il peut s'agir d'un individu qui procède régulièrement à des envois de fonds en espèces vers quelques destinataires, tous situés dans le même pays à risque.

Des recherches sur cet individu montrent que le total de ses envois atteint des montants très supérieurs à ses revenus connus.

Des recherches sur les bénéficiaires montrent qu'ils reçoivent d'autres transferts de la part d'autres personnes physiques présentant le même profil que le premier expéditeur (adresse, lieu d'expédition, faibles revenus connus...)

Dans le cas des bénéficiaires :

Il peut s'agir d'un bénéficiaire unique, établi dans un pays à risque, qui reçoit en un laps de temps court de nombreux envois de fonds, pour des montants totaux conséquents, de la part de plusieurs expéditeurs résidant tous dans le même périmètre géographique.

Des recherche sur les expéditeurs nouvellement identifiés montrent qu'ils adressent des fonds à une poignée de destinataires résidant tous dans la même zone du même pays à risque.

Cas n°9

Un groupe de 65 personnes, pour la plupart de nationalité française et domiciliées en Bretagne, a émis près de 150 transferts d'espèces par mandats depuis la ville de Rennes, à destination de la capitale d'un pays d'Amérique du Sud à risque en matière de trafic de stupéfiants avec l'Europe. Le total des opérations atteint 361 k€ en 18 mois. Les montants individuels sont élevés compte-tenu du profil socio-économique des expéditeurs, et les modalités d'envoi par fractionnement témoignent d'une volonté de contourner la vigilance des sociétés de transmission de fonds. Les transferts identifiés permettent d'établir un lien entre d'une part la majorité des expéditeurs, dont plusieurs sont mis en cause dans le cadre d'infractions à la législation sur les stupéfiants, et d'autre part un ensemble de 49 destinataires. Les recherches menées laissent supposer que les flux financiers relevés pourraient trouver leur origine dans un trafic de produits stupéfiants entre l'Amérique du Sud et la France métropolitaine, réalisé en bande organisée.

La gestion de PME et la fraude comptable

La gestion de PME permet de blanchir le produit de tout crime ou délit en utilisant la fraude comptable, la fraude fiscale et l'abus de bien social.

Cas n°10

Une société de production musicale est domiciliée dans un quartier sensible, connu pour abriter d'importants trafics de stupéfiants. Elle produit des artistes de la scène rap. Dans ses déclarations fiscales, la société présente des comptes d'exploitation cohérents. En revanche, l'analyse de ses flux bancaires révèle que le fonctionnement de la société diffère sensiblement des chiffres déclarés à l'administration fiscale.

Ses recettes correspondent à son activité. Elles proviennent essentiellement d'un distributeur musical, intermédiaire entre les maisons de production et les réseaux de distribution grand public, ainsi que de la SACEM. A l'inverse, la structure de ses dépenses ne reflète pas les charges d'exploitation attendues de ce type de société. Les charges ne mentionnent aucune rémunération d'artistes. Les salaires ne totalisent que 15 k€ par an alors que la société déclare trois salariés. Les paiements fournisseurs ne représentent que 30 k€ par an, dont l'essentiel vers une entité d'un secteur sans rapport avec la production musicale. En revanche, la société transfère environ 500 k€ par an vers des comptes d'épargne, dont la moitié en placements sur des comptes à terme. La société affiche également des dépenses par cartes bancaires, d'environ 75 k€ par an, correspondant à des dépenses d'agrément et de loisirs pour le gérant et ses proches. Des retraits d'espèces élevés sont également constatés.

Les comptes personnels du gérant présentent un fonctionnement atypique. Ils n'affichent aucune dépense courante. Les fonds reçus de la société sont placés sur des contrats d'assurance-vie et des comptes d'épargne. Son frère, se disant salarié de la société, reçoit des transferts de fonds en espèces de la part de tiers qui avaient auparavant reçu des paiements de la société.

La faiblesse des opérations identifiées au débit des comptes de la société et de son gérant suggère qu'ils utiliseraient des fonds hors du circuit bancaire pour régler une partie de leurs charges. Les investigations de Tracfin ont rapidement établi que la famille du gérant était notoirement connue pour trafic de stupéfiants, et impliquée dans des règlements de compte à l'arme à feu. Il est probable que les comptes de la société soient utilisés pour blanchir le produit d'un trafic de stupéfiants, en injectant des fonds d'origine douteuse dans une activité légale.

LES FILIÈRES D'IMMIGRATION CLANDESTINE UTILISENT LES ESPÈCES ET LES MANDATS CASH

Tracfin constate l'augmentation du nombre de dossiers portant sur des soupçons d'infraction à la législation sur les étrangers et de participation à des circuits d'immigration clandestine. Ces filières diffèrent notablement dans leur degré de structuration. Si certaines sont très organisées, d'autres apparaissent très éclatées, voire relèvent d'initiatives individuelles.

Cas n°11

Monsieur et Madame X sont originaires du Proche-Orient, mais domiciliés en France. En quatre ans, ils ont reçu de nombreux transferts d'espèces :

- près de 500 k€ en 250 mandats de la part d'un seul expéditeur, établi en bordure d'une zone de conflit au Proche Orient.

- près de 120 k€ en 60 mandats, la plupart émis par des personnes physiques de pays limitrophes à la zone de conflit.

Ces transferts n'ont pas de justifications et sont incohérents avec le train de vie de Monsieur et Madame X.

De plus, Monsieur X encaisse ces mandats dans plusieurs villes du territoire français, ainsi qu'à l'étranger, dans des villes d'Europe du Nord. Son activité bancaire révèle de fréquents déplacements, tant sur les frontières méditerranéennes de l'Europe que dans les villes de pays situés plus au nord.

L'enquête judiciaire a révélé que ces mandats de transferts d'espèces entre le Proche Orient et l'espace Schengen s'inscrivaient dans le cadre de la mise en œuvre d'un circuit d'immigration clandestine.

Cas n°12

Monsieur Y, originaire d'Asie du Sud, vit dans une cité du nord de l'Ile-de-France. Il ressort comme salarié d'une société de commerce de détail de textile et d'habillement sur les marchés. Il est connu des services de police pour des faits de travail dissimulé. Son épouse, de nationalité française, est femme de ménage.

En un an, alors que Monsieur Y a déclaré à l'administration fiscale des salaires à hauteur de 14 k€, il a perçu 200 k€ de flux créditeurs sur ses comptes bancaires, dont 120 k€ en chèques et 60 k€ en espèces. La majorité des chèques ont été émis par des PME du secteur du BTP. Monsieur Y reçoit également des virements ou des chèques de particuliers issus du même pays d'origine que lui.

Au débit, Monsieur Y affiche sur la même période près de 30 k€ de dépenses auprès de voyagistes et de transporteurs aériens, ce qui est incompatible avec ses revenus déclarés. L'enquête a démontré que les billets d'avion avaient tous été achetés pour des tiers. De plus, Monsieur Y a procédé à 25 transferts d'espèces d'environ 1 000 € chacun, dont la moitié vers son pays d'origine.

L'enquête judiciaire a permis de confirmer la participation de Monsieur Y à un délit d'aide à l'entrée et au séjour irréguliers.

LA VULNÉRABILITÉ DU SECTEUR DES JEUX D'ARGENT ET DE HASARD

Le secteur des jeux d'argent et de hasard est toujours fortement exposé aux risques de blanchiment d'espèces frauduleusement acquises. Tous les acteurs du secteur sont concernés.

Les opérateurs de paris hippiques, de paris sportifs et de jeux de grattage constituent une préoccupation constante de Tracfin. Le Service reçoit et traite chaque année des cas de rachats de tickets gagnants, ou de paris sportifs répétés sur des compétitions à faible cote, pouvant impliquer la complicité des détaillants.

Les casinos restent eux aussi vulnérables. En 2016, Tracfin a traité des dossiers de montants importants, en particulier du fait de filières asiatiques.

Cas n°13

Monsieur Z se déclare sans emploi mais possède une affaire personnelle d'artisan-commerçant active dans le commerce de véhicules d'occasion. Il est connu des services de police pour vol et recel. Ses comptes bancaires sont exclusivement alimentés de versements de la CAF, systématiquement retirés en espèces, et ne présentent aucune dépense courante. Suite à un contrôle fiscal, il est redevable de 140 k€ à l'administration fiscale.

En deux ans, Monsieur Z a gagné un total de plus de 610 K€ en jouant dans plusieurs casinos du territoire français, à la fois aux machines à sous et aux jeux de table. Compte tenu des taux de redistribution de ces jeux sur longue période, pour être en mesure de gagner une telle somme, l'intéressé a dû miser au moins 670 K€ en deux ans. Or les mises enregistrées par les casinos au nom de Monsieur Z ne s'élèvent qu'à 14 K€.

Monsieur Z n'a joué qu'en espèces et a sciemment multiplié les mises inférieures au seuil de 2 000 € afin d'éviter les prises d'identité. Il a été aidé en cela par les machines à sous et les jeux de roulette électronique, qui peuvent être alimentés directement en espèces (machines dites *bill acceptors*). L'absence de traçabilité des mises limite les travaux d'investigation du Service

L'analyse de ses comptes bancaires atteste qu'aucun de ses gains, perçus en espèces, n'a été déposé sur un compte bancaire (du moins en France). L'absence de bancarisation de ses mises ou de ses gains laisse soupçonner une origine délictueuse des fonds détenus en espèces, qu'il s'agisse d'activités non déclarées (Monsieur Z est redevable de 140 k€ à l'Administration fiscale) ou d'activités criminelles. Monsieur Z commet un délit de blanchiment par le jeu.

Tracfin a également traité plusieurs dossiers concernant des membres de la communauté asiatique. Ils engagent au casino de très fortes sommes en espèces, et affichent des pertes en proportion, sans commune mesure avec leurs revenus déclarés ou l'activité de leurs comptes bancaires.

Cas n°14

Madame W et Madame H sont toutes deux d'origine asiatique. Madame W a la nationalité française. Elles fréquentent les mêmes établissements de jeu et se connaissent. La première a émis quelques chèques de montant modeste en faveur de la seconde.

Le compte bancaire de Madame W présente un fonctionnement incohérent. Alors qu'elle et son époux ne déclarent que 15 k€ de revenus annuels, le compte bancaire de Madame W affiche une activité intense. En deux ans, elle a reçu :

- 300 k€ de dépôts d'espèces ;
- 50 k€ de virements issus de tiers ;
- 50 k€ de chèques.

Sur la même période, au débit, le compte affiche :

- 175 k€ de paiements par carte bleue au sein de divers casinos ;
- 130 k€ de retraits d'espèces (dont 35 k€ auprès de distributeurs logés au sein de casinos) ;
- 100 k€ de chèques émis.

Madame H, quant à elle, ne déclare aucun revenu et son compte bancaire ne présente quasiment aucune activité.

Le fonctionnement inhabituel de leurs comptes bancaires se double d'une activité intense de jeu au casino, ayant cumulé chacune près de 500 visites en deux ans dans différents établissements. Les sommes transitant sur les comptes de Madame W ne peuvent expliquer celles engagées au jeu.

En deux ans, Madame W a totalisé 280 k€ de pertes aux jeux de table. Elle a misé un total de 1,2 M€, dont 1 M€ en espèces pour des achats massifs de jetons. Elle a retiré 920 k€ de gains.

Sur la même période, Madame H a totalisé des pertes de 1 M€. Elle a joué exclusivement en espèces, changeant pour 1,3 M€ de jetons à l'achat, et ne convertissant que 0,3 M€ de jetons en gains. Elle a de plus procédé à des dépôts et retraits de jetons pour un total de 800 k€.

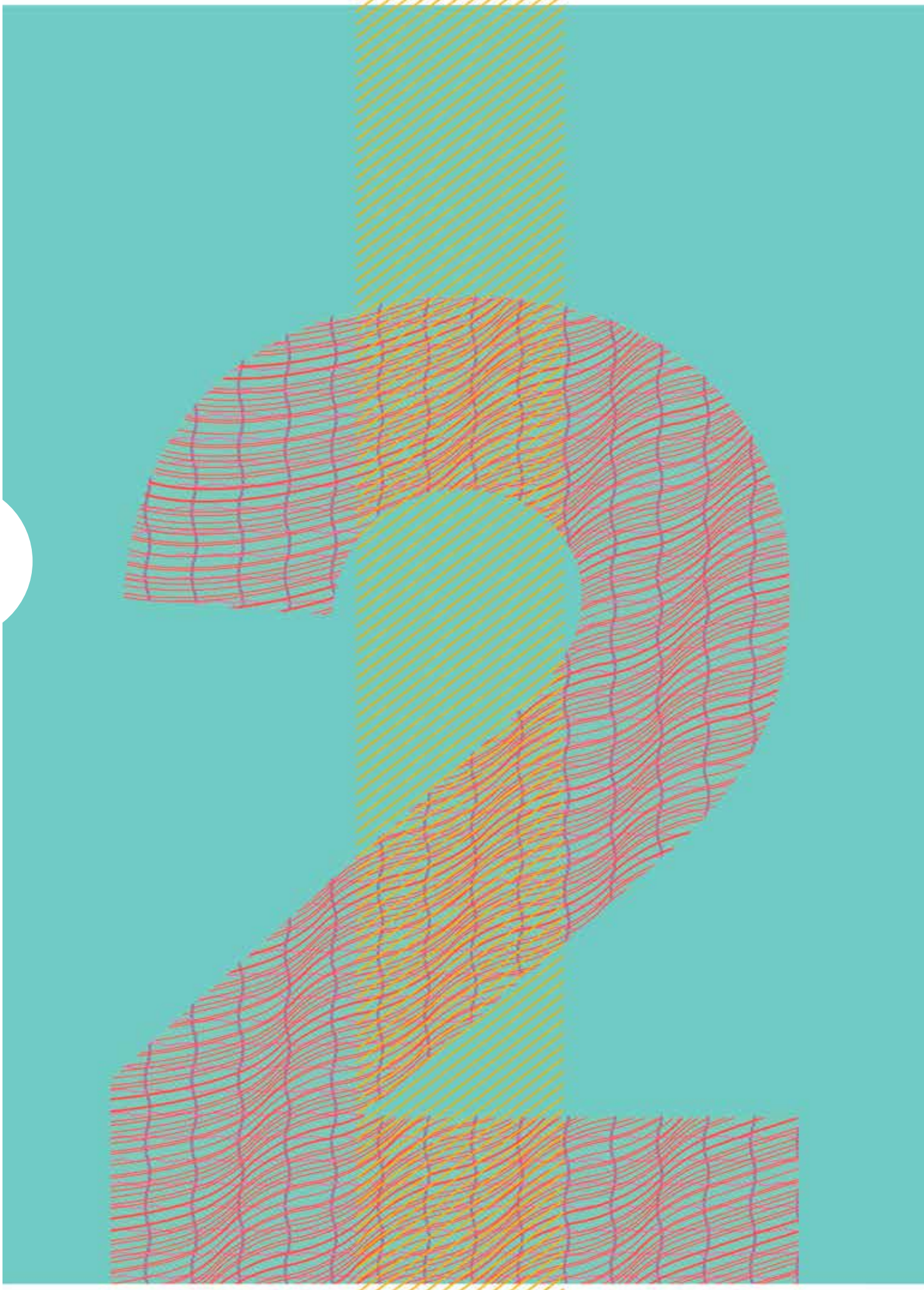
Différents éléments suspects sont ainsi mis en avant :

- la manipulation par Madame W d'un volume conséquent d'espèces, à l'origine inconnue, relevée, tant dans le fonctionnement de ses comptes bancaires, que dans son activité de jeu au sein du casino ;
- la faiblesse de l'activité bancaire de Madame H, qui

dispose de comptes peu mouvementés et qui n'engage quasiment pas de dépenses liées à la vie courante ;

- une activité de jeu intense dans les casinos, alors que les deux intéressées n'ont aucune ressource officielle ;
- une déconnection entre les mouvements enregistrés au débit de leurs comptes et les transactions engagées au casino : notamment l'absence de sortie d'espèces à hauteur du montant des pertes.

Ce brassage de numéraire par Mesdames W et H s'expliquerait par le fait que ces masses de liquidités ne leur appartiendraient pas en propre. Leur perte finale peut s'expliquer si on considère qu'elles distribuent régulièrement, à d'autres joueurs complices, les jetons en leur possession. Les sommes manipulées pourraient ainsi être issues d'agissements occultes, générateurs de numéraire, et le casino utilisé comme une banque occulte afin de blanchir les fonds apportés par la communauté et de les restituer à leur propriétaire.



LA LUTTE CONTRE LE TERRORISME ET SON FINANCEMENT MOBILISE TOUS LES ACTEURS DE L'ÉTAT

En 2016, la lutte contre le terrorisme et son financement a confirmé sa montée en puissance. En la matière, Tracfin a traité un volume d'informations en constante augmentation :

– 1 177 déclarations de soupçon liées au financement du terrorisme ont été reçues et analysées, soit une augmentation de 47% par rapport à l'année 2015.
– 396 investigations ont donné lieu à une note de transmission (+ 121% par rapport à 2015) parmi lesquelles :

- *352 notes ont été adressées aux différents services de renseignement ;*
- *44 notes ont été adressées à l'autorité judiciaire ou aux services de police judiciaire en charge de la lutte contre le terrorisme.*

Les notes d'information sur le financement du terrorisme issues des investigations de Tracfin alimentent les services de renseignement, les services de police et les tribunaux de grande instance. Au plan judiciaire, Tracfin entretient une relation de coopération étroite avec la section antiterroriste du parquet de Paris, principal destinataire des enquêtes menées par le Service.

Les informations transmises à l'autorité judiciaire en 2016 reflètent les principaux schémas de financement du terrorisme observés par le Service :

– *La détection des signaux faibles de radicalisation et les combattants sur le départ.*
– *La problématique des returnees : les combattants de retour de la zone de conflit.*
– *Le financement du terrorisme par les réseaux de collecteurs.*
– *Le financement du terrorisme par le biais des associations.*

Outre les enquêtes de profilage menées sur les individus en lien avec les auteurs des attentats ou tentatives d'attentats survenus en France et en Europe depuis 2015, les dossiers judiciarisés émanant de Tracfin concernent principalement des cas de collecteurs de fonds servant d'intermédiaire entre émetteurs et combattants sur zone, par la concentration puis la redistribution de transferts d'espèces internationaux, ainsi que des dossiers de financement par le biais d'associations à vocation culturelle ou cultuelle.

Ces menaces terroristes recourent à des canaux financiers variés. Outre les flux bancaires traditionnels sur lesquels Tracfin possède une visibilité importante, le financement du terrorisme fait intervenir des produits et acteurs alternatifs. Les cartes prépayées, pour lesquelles le législateur a adapté le cadre réglementaire à la suite des attentats de 2015, sont utilisées pour l'envoi de fonds vers des réseaux de collecteurs. Ces derniers s'adressent principalement aux sociétés de transmission de fonds pour récolter et retirer des fonds en espèces. De même, l'expansion des plateformes de financement participatif a bénéficié à des mouvements radicalisés qui ont profité de leur banalisation. La création de cagnottes en ligne prétextant de faux projets ont permis de récolter des dons destinés in fine à soutenir matériellement ou financièrement des filières terroristes.

LES COMBATTANTS ET/OU LA DÉTECTION DES SIGNAUX FAIBLES DE RADICALISATION

En matière de lutte contre le terrorisme, le renseignement financier s'attache à la détection de signaux faibles. La préparation d'actes terroristes s'effectue par le biais de micro-financements difficiles à tracer. Les flux caractéristiques d'un passage à l'acte ne se démarquent que rarement des volumes de micro-transactions légitimes.

Les éléments proprement financiers doivent être recoupés avec des critères comportementaux. L'accent est mis sur le détail de petites opérations concernant des individus présentant des signes extérieurs de radicalisation ou de départ imminent pour une zone de combat.

Tracfin a diversifié ses formats de transmission aux autorités compétentes pour répondre au mieux à cet enjeu. Outre les transmissions à l'autorité judiciaire, le Service a développé des transmissions dites « flash » pour répondre de manière rapide et précise aux urgences et besoins ponctuels des services de renseignement et de police partenaires. Ces transmissions « flash » portent sur des opérations financières ou des individus bien déterminés. Depuis leur mise en place courant 2016, le Service a effectué 80 transmissions de ce type, soit près de 20% des transmissions totales en matière de lutte contre le financement du terrorisme en 2016. Ce chiffre a vocation à augmenter de manière substantielle en 2017.

Cas n°15 : Détection d'un départ pour le djihad

Un déclarant informe le Service de la volonté d'un individu né en 1995 de donner procuration à un parent sur son compte bancaire avant de le clôturer. Il explique qu'il part à l'étranger pour des raisons personnelles et une durée indéterminée. Le parent de l'individu précise, lors de la clôture définitive du compte, que ce dernier ne reviendra pas en France. L'analyse des comptes de l'individu révèle de nombreuses dépenses pour des équipements de vie en extérieur et de camping avant clôture des comptes épargne et courant.

Critères d'alerte :

- Fermeture soudaine de l'ensemble des comptes bancaires de l'individu
- Départ pour une durée et une zone indéterminée
- Achats de matériel de vie en extérieur
- Explications évasives sur les motifs et la destination finale du voyage
- Âge de l'individu

Cas n°16 : Détection d'un processus de radicalisation

Un déclarant contacte le Service pour lui faire part d'un changement récent de comportement d'un client souhaitant quitter la France pour s'installer dans un pays d'Afrique du Nord dont il n'est pas originaire. L'individu, salarié, a perçu une somme importante de sa société après avoir procédé à une rupture conventionnelle de contrat. Il se serait récemment converti, a changé d'apparence physique et refuse tout contact physique avec les femmes employées par le déclarant. Il effectue également des virements au bénéfice d'une association cultuelle et a demandé des informations sur les modalités de transferts de fonds vers un pays étranger.

Les recherches de Tracfin ont rapidement établi que l'individu était signalé « S » dans le fichier des personnes recherchées.

Critères d'alerte :

- Conversion religieuse rapide et/ou démonstrative
- Changement d'apparence physique de l'individu
- Projet de départ dans un pays d'Afrique du Nord

Cas n°17 : Détection de virements suspects vers des individus radicalisés

Tracfin est informé qu'un individu a déposé 15 000 € en espèces dans une agence bancaire sans donner de précisions sur l'origine des fonds. Le lendemain il effectue un virement du même montant en Belgique à destination d'une personne physique, accusée dans ce pays de meurtre en lien avec des actes terroristes. Ce ressortissant belge aurait apporté un soutien logistique à l'auteur d'une attaque terroriste ; il est en détention provisoire depuis son extradition de France.

Critères d'alerte :

- Dépôt d'espèces important
- Virement au bénéfice d'une personne placée en détention
- Liens avec des individus connus en sources ouvertes pour appartenir à une mouvance terroriste

LA PROBLÉMATIQUE DES *RETURNEES*

Le montage d'une opération de retour de zone de combat nécessite plusieurs milliers d'euros. L'entourage proche de l'individu désireux de revenir en France doit mobiliser des fonds en conséquence.

Tracfin collecte du renseignement sur des opérations douteuses observées sur les comptes des membres de l'environnement familial et amical d'individus présents sur zone de combat. Ces opérations prennent diverses formes. Les plus fréquentes correspondent à des décaissements en espèces du produit de ventes de voiture ou de maison, ou de clôture de contrat d'assurance-vie. Les professionnels assujettis exercent une vigilance accrue sur la famille et les proches de personnes ayant déjà fait l'objet d'un droit de communication de la part de Tracfin pour soupçon de départ en zone de djihad.

Le nombre de *returnees* reste relativement faible ; c'est pourquoi Tracfin recense peu de cas de financement de retour, en France, de combattant djihadistes. Néanmoins, Tracfin a enquêté sur des récoltes de fonds par le biais de cagnottes en ligne créées pour financer le retour de combattants. Le lien redirigeant vers l'adresse de la cagnotte était diffusé sur les réseaux sociaux. Un droit de communication auprès de la plateforme de cagnottes en ligne a permis à Tracfin de récupérer l'identité du créateur de la cagnotte et d'identifier les donateurs.

LES RÉSEAUX INTERNATIONAUX DE COLLECTEURS

Le territoire conquis par Daech représentait sa première source de financement, à travers les butins de guerre, l'extorsion des populations, l'exploitation des ressources naturelles, la taxation des flux commerciaux et les trafics. A l'heure où Daech enregistre des pertes militaires, son territoire se rétrécit et ses ressources financières internes se tarissent. Le mouvement tente de compenser partiellement ces pertes de revenus par un recours toujours soutenu aux financements extérieurs. Ces flux financiers internationaux peuvent révéler d'éventuels redéploiements géographiques du mouvement.

LE RÔLE ET L'ORGANISATION DES RÉSEAUX DE COLLECTEURS

Les principaux architectes des flux financiers étrangers collectés au profit de Daech sont appelés les collecteurs. Ce sont des facilitateurs financiers qui proposent un ensemble de services, parmi lesquels :

– garder l'argent d'un combattant étranger voyageant de/vers les pays de l'arc de crise afin de réduire le risque lié au franchissement de la frontière avec des espèces ;
– sécuriser le montant dû à un passeur par un combattant en réglant la somme lorsque la frontière a été franchie ;
– recevoir des fonds au nom d'un bénéficiaire qui n'a pas de carte d'identité valide ou pour qui il serait trop risqué de la dévoiler ;
– apporter de l'argent directement vers une zone de combat pour en faire bénéficier un combattant ;
– envoyer, par un système de compensation de type *hawala*, un montant vers une zone de combat.

Les membres français du groupe Etat islamique organisent l'acheminement des fonds en fournissant à leurs proches restés en Europe, par le biais d'applications mobiles, le nom d'un collecteur et les modalités du transfert à opérer (commissions, agences de transfert). Les fonds ainsi obtenus grâce à l'entourage sont consacrés aux dépenses quotidiennes sur place.

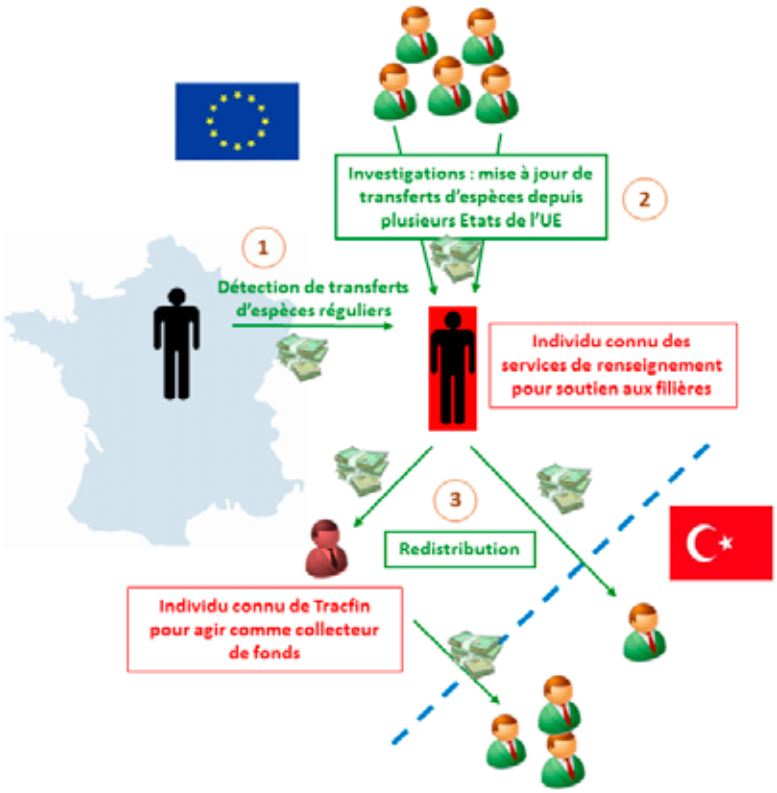
En 2016, Tracfin a initié une investigation de grande ampleur en analysant plusieurs milliers d'opérations de transferts d'espèces, pour mettre à jour des réseaux de collecteurs. Les données analysées, provenant de droits de communication émis par Tracfin auprès des principaux opérateurs de transmission de fonds, révèlent des modes opératoires similaires entre les différents envois à destination des collecteurs.

Ces caractéristiques communes permettent de dégager une typologie :

– Les expéditeurs réunissent la somme à envoyer en utilisant plusieurs sources de micro-financements.
– Ils effectuent dans la plupart des cas un envoi unique, ou quelques envois peu nombreux. Les envois sont le plus souvent vers des pays frontaliers de la zone de conflit au Proche Orient.
– Les collecteurs reçoivent ainsi une multiplicité de flux de la part de nombreux particuliers sans liens entre eux ni cohérence, depuis des pays variés, avec une prédominance de pays européens.
– Les flux ont pour destination finale les pays de l'arc de crise au Levant.

Cas n°18 : Mise à jour d'un réseau de collecteurs

L'attention de Tracfin est portée sur des opérations de transferts d'espèces réguliers entre deux individus résidant dans deux pays différents de l'UE. L'un des deux individus est connu des services de renseignement pour son implication dans des filières syriennes d'acheminement de combattants et son soutien logistique à l'État islamique. L'analyse des opérations financières de ce dernier révèle qu'il est le bénéficiaire de nombreux transferts d'espèces en provenance de plusieurs pays européens, qu'il redistribue au profit de tiers dont certains résident en Turquie. Un autre de ces tiers, résident d'un pays de l'UE, est déjà connu du Service pour être un collecteur de fonds à destination de la Turquie.

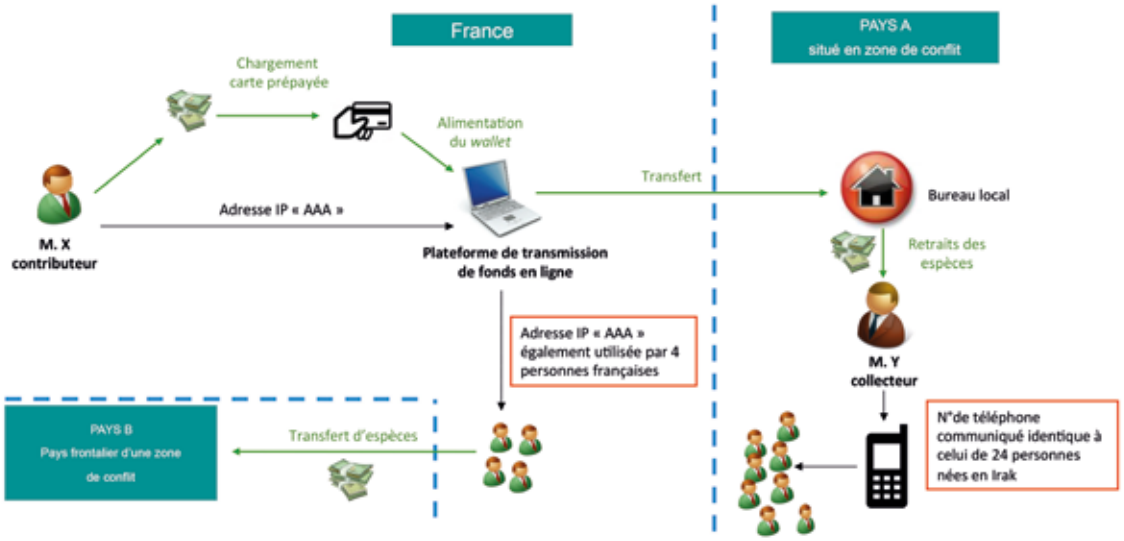


Cas n°19 : Alimentation d'un réseau de collecteurs à partir de cartes prépayées

Monsieur X se procure une carte prépayée qu'il recharge à trois reprises à partir d'espèces. Avec les coordonnées de la carte prépayée, il procède (via internet) à une opération de transfert d'espèces, à destination de Monsieur Y situé dans un pays en zone de conflit (pays A), qui retire les fonds en espèces dans un bureau local. Le numéro de téléphone indiqué par Monsieur Y lors du retrait des fonds est identique à celui utilisé par 24 autres personnes, toutes nées dans le pays A.

Par ailleurs, l'adresse IP à partir de laquelle la transaction a été effectuée en ligne par Monsieur X a également servi à quatre autres personnes qui ont effectué des opérations de transferts d'espèces à destination de bénéficiaires localisés dans le pays B, pays frontalier d'une zone de conflit.

La multiplicité des identités découvertes pour un même numéro dans le pays A et pour une même adresse IP en France indique probablement le recours à de fausses identités à des fins de discrétion. Les cartes prépayées apparaissent particulièrement vulnérables aux fraudes à l'identité.



Cas n°20 : Le réseau M

Fin 2015, la section antiterroriste du Parquet de Paris a ouvert une enquête préliminaire à partir d'un signalement Tracfin. Cette enquête a visé les activités de collecteur de fonds pour l'Etat islamique de Monsieur M, poursuivi pour :

- participation à une association de malfaiteurs en vue de commettre des actes de terrorisme (art. 421-2-1 du Code pénal) ;
- financement du terrorisme (art. 421-2-2 du Code pénal).

Monsieur M a collecté des fonds en provenance de nombreux pays européens par l'intermédiaire de sociétés de transmission de fonds pour ensuite les reverser à des djihadistes de l'Etat islamique.

Entre mai 2014 et août 2015, vingt-quatre Français lui ont envoyé des fonds pour un montant total de 40 300 dollars.

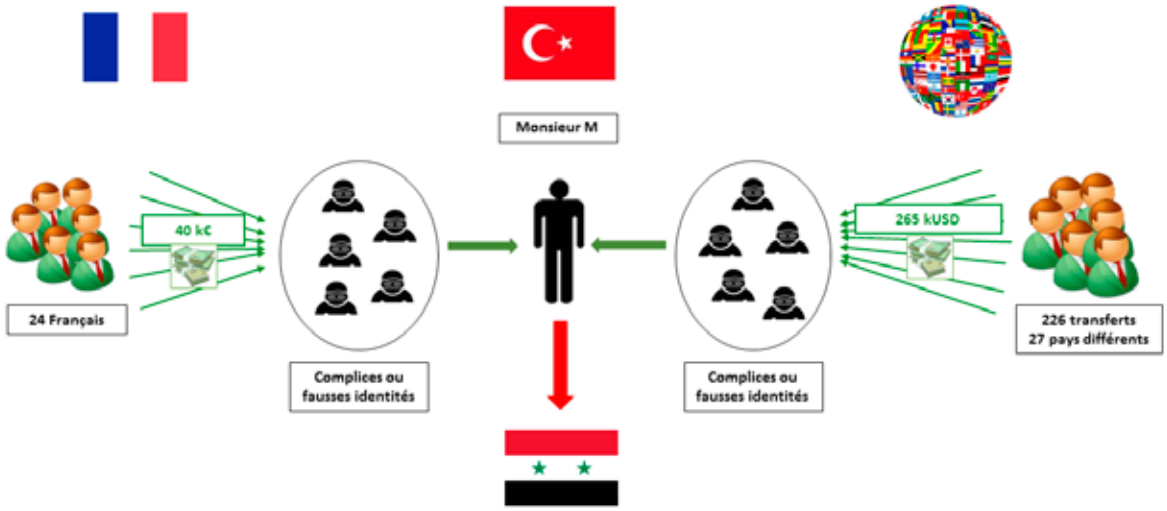
Monsieur M a développé son réseau avec l'aide de nombreux complices ou en se masquant derrière de fausses identités.

Son impact, significatif sur l'ensemble des filières européennes, a été l'un des éléments déclencheur de l'action de nombreux services sur la thématique des collecteurs.

L'implication de Monsieur M comme courtier du djihad a été confirmée par les auditions des expéditeurs mais aussi par l'exploitation de matériel saisi. Les transferts d'argent étaient réalisés par Monsieur M lui-même (ou affiliés), qui effectuait régulièrement des allers-retours entre la Turquie et la Syrie et prélevait une commission de 4 % sur chacune des transactions.

Au-delà de la France, Tracfin a constaté la présence de 226 transferts envoyés depuis 27 pays différents pour une somme globale de 265 000 dollars, soit un bénéfice pour Monsieur M d'environ 11 000 dollars en un an.

Monsieur M est aujourd'hui inscrit sur la liste des sanctions de l'*Office of Foreign Assets Control* (OFAC) et son cas a posé les jalons d'initiatives européennes notamment favorisées par l'implication d'Europol.



LA DÉTECTION DES RÉSEAUX DE COLLECTEURS A RENFORCÉ UNE DYNAMIQUE DE COOPÉRATION EFFECTIVE ENTRE SERVICES

La cartographie des réseaux de collecteurs résulte d'une coopération interservices effective et aussi d'une meilleure collaboration avec les opérateurs du secteur privé.

Les partenariats institutionnels

Au sein de la Communauté du renseignement :

Par le suivi des réseaux de collecteurs et la détection d'expéditeurs français, Tracfin participe à l'appréhension des menaces terroristes au bénéfice de la communauté française du renseignement. Le Service est mis à contribution au sein d'une cellule interservices de mutualisation des renseignements au sein de la DGSI (Direction Générale de la Sécurité Intérieure).

Avec l'autorité judiciaire :

Un renforcement du partenariat entre Tracfin et l'autorité judiciaire a été mené, grâce à de nouvelles modalités de collaboration. En 2016, Tracfin a mis en place des supports de transmission d'information standardisés afin de faciliter les investigations du parquet sur les affaires en cours de traitement.

Avec les homologues internationaux de Tracfin :

A l'échelle internationale, la prise en compte de ce micro-financement est encore disparate au sein des CRF. La France et la Belgique ont développé une politique d'échange sur le sujet. En parallèle, Tracfin a recours au réseau des CRF pour transmettre à ses partenaires des données sensibles.

Les professionnels assujettis

Des partenariats particuliers ont été spécialement initiés au cours de l'année 2016 afin que les partenaires privés puissent répondre avec précision et célérité aux demandes de Tracfin. Les grands acteurs de la Place ont bénéficié, parfois en lien avec nos partenaires institutionnels, d'évaluation de menaces spécifiques à l'initiative en cours.

Outre les droits de communication exercés par Tracfin, ces assujettis ont pu faire remonter par le biais de leurs déclarations de nouveaux soupçons. De nouvelles routes financières ont pu ainsi être identifiées.

LES ASSOCIATIONS SOUPÇONNÉES DE FINANCEMENT DU TERRORISME

L'analyse par Tracfin des déclarations de soupçon de financement du terrorisme a fait remonter certaines associations comme points de convergence de flux financiers destinés à financer des réseaux djihadistes. A partir des signalements émis à l'attention de Tracfin, trois catégories d'associations peuvent être concernées :

– **Des associations à vocation humanitaire** : elles proposent d'apporter des aides matérielles, alimentaires ou médicales dans des zones déshéritées ou de conflit. Leur action officielle consiste à envoyer du personnel (médecins, infirmiers, humanitaires), des marchandises ou des sommes d'argent essentiellement à l'étranger.
– **Des associations culturelles** : leurs actions sont variées. Elles concernent l'achat de livres, l'organisation de conférence ou bien la mise en place de cours de langue ou de soutien scolaire.
– **Des associations cultuelles** : leur objet déclaré est la gestion ou la construction de lieux de culte.

Les associations signalées à Tracfin pour soupçon de financement du terrorisme sont essentiellement localisées en région parisienne mais également en région PACA, en région Rhône-Alpes et dans l'Est de la France. Les modes de financement de ces associations reposent principalement sur les dons provenant de particuliers appartenant à la communauté visée par l'objet associatif. Pour les associations à dimension régionale, les particuliers ressortent généralement du tissu local.

Des financements provenant de l'étranger peuvent ponctuellement être signalés en lien avec le fonctionnement de comptes associatifs gérant des lieux de culte connus pour héberger des éléments radicaux.

Eventuellement, certaines associations peuvent bénéficier de financement public, sous la forme de subventions accordées dans le cadre de leur activité officielle.

L'étude des comptes bancaires de ce type d'associations révèle une opacité dans l'utilisation des fonds, notamment lorsqu'il s'agit d'associations à vocation humanitaire menant leurs actions à l'étranger. Les comptes permettent d'alimenter des personnes physiques ou morales situées à l'étranger sans qu'il soit possible d'établir un lien avec l'action humanitaire visée. De même, arguant de l'absence d'un système bancaire fiable dans la zone d'action, les associations procèdent à des retraits d'espèces importants pouvant atteindre plusieurs dizaines de milliers d'euros, voire plus.

Plusieurs modes de fonctionnement interviennent également dans l'opacification des circuits financiers empruntés par les associations visées :

– le recours à des plateformes de paiement situées à l'étranger ;
– les flux croisés entre associations en France et à l'étranger ;
– des pratiques relevant de l'abus de confiance.

Cas n°21 : Financement d'un lieu de rassemblement par le biais d'une association fréquentée par des individus radicalisés

Une SCI gérée par Monsieur A sollicite et obtient un prêt destiné à financer une acquisition immobilière. Le règlement du solde de l'opération d'achat n'est pas réglé par la SCI mais par l'association B, active dans les domaines éducatif, social et culturel auprès de jeunes d'une communauté ciblée. Les ressources de l'association B proviennent de droits d'entrée, de dons mais aussi de subventions publiques. Or, certains membres du bureau de l'association B sont connus par les services de renseignement pour appartenir à la mouvance radicale. Sur la période précédant l'opération d'achat immobilier, le compte de l'association B a été alimenté à hauteur de plusieurs centaines de milliers d'euros sous forme de virements, remises de chèques et versements d'espèces émanant, pour les plus gros montants, des membres du bureau de l'association. Des virements proviennent également de Monsieur A par l'intermédiaire d'une troisième association et d'une société commerciale. Le bien acquis pourrait servir de lieu de rassemblement de groupes radicaux.

Cas n°22 : Soutien logistique et financier à Daech sous couvert d'aide humanitaire par l'intermédiaire d'une cagnotte en ligne

Une association F, présidée par Monsieur X, a pour objet l'aide humanitaire et l'aide au développement dans des pays en voie de développement. Monsieur X et les membres de son bureau, issus d'un Etat slave, sont soupçonnés d'adhérer aux idées d'un mouvement salafiste favorable au rétablissement du califat. Sous couvert d'aide humanitaire, l'association F soutiendrait financièrement et matériellement Daech au Levant. L'association F procède à une récolte de fonds par l'intermédiaire d'une cagnotte en ligne associée à un compte ouvert dans l'Etat d'origine de Monsieur X. Les fonds récoltés proviennent de ce pays et sont intégralement retirés en espèces.

LA LUTTE CONTRE LA CORRUPTION ET LA LUTTE CONTRE LES FRAUDES FISCALES ET SOCIALES SUSCITENT DES ATTENTES FORTES

La lutte contre la corruption et la lutte contre les fraudes fiscales et sociales sont au cœur des missions de long terme de Tracfin. Elles suscitent une attente forte compte-tenu du contexte national et international :

- *En matière de corruption, du fait de la situation dégradée de certains pays victimes de pratiques prédatrices, de la médiatisation de dossiers importants et des travaux de l'OCDE qui s'apprête à célébrer les vingt ans de la convention de 1997.*
- *En matière de fraude fiscale, du fait de la nécessité de redresser les comptes publics et de lutter contre la grande fraude fiscale transnationale, avec en particulier la mise en place à partir de 2017 de l'échange automatique d'informations fiscales.*
- *En matière de fraude sociale, pour contribuer à préserver l'équilibre financier et donc la pérennité des organismes de sécurité sociale.*

LUTTE CONTRE LA CORRUPTION : LES DOSSIERS INTERNATIONAUX NE DOIVENT PAS OCCULTER LES RISQUES PROPRES AU TERRITOIRE FRANÇAIS

La lutte contre les manquements à la probité est portée par un contexte international qui met l'accent sur la corruption dans le cadre des transactions commerciales à l'étranger :

- Le groupe de travail dédié de l'OCDE, mis en place dans le prolongement de la convention de 1997 et chargé d'auditer les dispositifs anticorruption des pays signataires, se concentre sur la corruption dans les transactions commerciales internationales (principalement les infractions de corruption active et passive et de trafic d'influence).
- En France, la loi n°2016-1691 du 9 décembre 2016 (dite loi Sapin 2) a été en partie créée pour des motifs relevant du commerce international. Elle vise à doter la France d'un dispositif anticorruption comparable à celui d'autres pays occidentaux, de manière à ce que ceux qui disposent des législations les plus étoffées ne puissent plus prendre prétexte de la faiblesse de la législation française pour poursuivre les entreprises françaises.

Pour autant, la France est aussi vulnérable aux manquements au devoir de probité commis sur le territoire national par des personnes exerçant une fonction publique : élus[1], personnes dépositaires de l'autorité publique ou personnes en charge d'une mission de service public. En sus des délits de corruption et de trafic d'influence, ces manquements incluent les infractions de favoritisme, de prise illégale d'intérêt ou de détournement de biens.

Avec une cinquantaine de dossiers traités par an, Tracfin mène une action résolue dans les deux directions, tant à l'international que sur le territoire français.

LA LOI N°2016-1691 DU 9 DÉCEMBRE 2016 (DITE LOI SAPIN 2)

La loi Sapin 2 comporte plusieurs innovations :

- Création du délit de trafic d'influence actif et passif à destination d'un agent public dans un Etat étranger.
- Elargissement de la compétence territoriale et extraterritoriale de la loi française.
- Cause d'irresponsabilité en faveur du lanceur d'alerte.
- Peine de manquement au programme de mise en conformité (sanctions para-pénales prononcées par une agence dédiée : l'Agence française Anticorruption).
- Convention judiciaire d'intérêt public.

Elle crée une obligation de conformité anticorruption à portée territoriale et extraterritoriale, en phase avec l'extension des compétences territoriale et extraterritoriale de la loi pénale française. Elle permet de prévenir un fait relevant de la compétence de la loi pénale et du juge pénal français, que les faits soit commis entièrement sur le territoire français, partiellement sur ce territoire, ou entièrement en-dehors de ce territoire. Elle facilite ainsi la poursuite des entreprises étrangères.

1 La 4ème directive transposée en droit français par l'ordonnance n°2016-1635 du 1er décembre 2016 étend la notion de Personnes Politiquement Exposées (PPE) aux PPE nationales, alors qu'elle ne concernait auparavant que les personnalités étrangères.

La loi Sapin 2 invite les entreprises à mettre en place un dispositif de lutte contre la corruption (OCA : Obligations de Conformité Anticorruption) et crée l'Agence Française Anticorruption (AFA), chargée de contrôler la bonne application de ce dispositif. Les entreprises concernées par les OCA sont les sociétés ou groupes de société ayant leur siège en France, et remplissant au moins un des deux critères : avoir un effectif de plus de 500 salariés, et/ou réaliser un chiffre d'affaires de plus de 100 M€[1].

Le dispositif anticorruption impose huit mesures aux entreprises concernées (art. 17 de la loi n°2016-1691) :

- Un code de conduite intégré au règlement intérieur ;
- Un dispositif d'alerte interne dédié, la loi créant un statut pour les lanceurs d'alerte.
- Une cartographie des risques de corruption sous forme d'une documentation formalisée et actualisée, permettant d'identifier, d'analyser et de hiérarchiser les risques.
- Des procédures d'évaluation de la situation des clients, des fournisseurs de premier rang et des intermédiaires, au regard de la cartographie des risques.
- Des procédures de contrôle comptable interne et/ou externe.
- Un dispositif de formation du personnel, en particulier les cadres.;
- Un régime disciplinaire permettant de sanctionner les salariés en cas de violation du code de conduite de la société.
- Un dispositif de contrôle et d'évaluation interne des mesures mises en œuvre.

1 Ces deux critères mériteraient d'être précisés, tant dans la méthode de dénombrement des salariés, que dans la définition du périmètre du chiffre d'affaires. De plus, la corruption n'est pas que le fait des grandes entreprises. Les petites sociétés en sont aussi les acteurs, soit de manière autonome, soit en tant qu'écran pour de grands groupes.

LA CORRUPTION PUBLIQUE ET PRIVÉE À L'INTERNATIONAL

La corruption d'Agent Public Etranger (APE)

Les délits liés à la corruption d'Agent Public Etranger sont définis par les articles 435-1 à 435-4 du code pénal. Ils sont issus de la loi du 30 juin 2000, entrée en vigueur le 29 septembre 2000, qui transposait les principales dispositions de la Convention de l'OCDE, et ont été précisés par la loi n°2013-1117 du 6 décembre 2013 et la loi n°2016-1691 du 9 décembre 2016.

A travers la tenue des comptes bancaires, les activités de *correspondent banking*, d'audit ou de certification comptable, les professionnels assujettis transmettent des soupçons étayés à Tracfin, qui font du Service un outil de qualité pour la détection de ces infractions.

Cas n°23

Une PME industrielle française cherche à vendre du matériel sensible à un client public d'Afrique de l'Ouest. Elle transfère 2 M€ dans ce pays vers les comptes de personnes morales non identifiées qui ne ressortent pas dans sa comptabilité en tant que fournisseurs.

Les modalités de l'opération constituent autant de critères d'alerte :

- Le total des transferts (2 M€) est excessivement élevé par rapport au chiffre d'affaires de l'entreprise française (5 M€).
- Les transferts unitaires n'ont jamais dépassé 150k€, montant correspondant à la limite de délégation de signature du directeur général sur les comptes bancaires de la société.
- Les entités destinataires des fonds sont inconnues des bases de données commerciales de leur pays. Elles ne sont pas reprises dans la comptabilité fournisseurs de l'entreprise française exportatrice.
- La comptabilisation des opérations s'étend sur une année et semble anormalement complexe, ventilant les montants sur différents comptes du plan comptable, normalement non destinés à ce type de transactions.

La société française donne des justifications peu convaincantes. Elle explique que ces transferts de fonds sont liés à la vente de matériel de communication. Les contrats qu'elle a présentés n'ont pas été mis en application et semblent fictifs. Il n'y en a pas trace ni dans les déclarations douanières de la société, ni dans ses opérations bancaires. L'enquête a établi que ces versements ont servi à la rémunération d'intermédiaires.

Le recours à un sous-traitant par un grand groupe

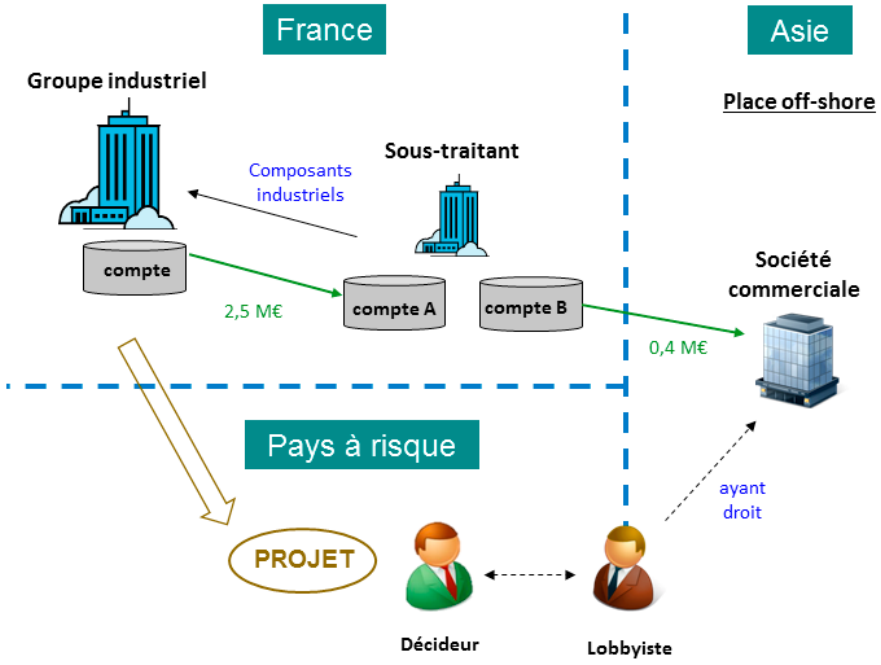
Les grands groupes soumis à des contraintes commerciales dans certains pays à risque peuvent chercher à externaliser les opérations de corruption auprès de sous-traitants plus discrets, sur lesquels ils exercent un contrôle de fait.

Cas n°24

Un groupe industriel français développe un projet dans un pays à risque en matière de corruption. Le groupe recourt à un sous-traitant spécialisé pour la fabrication de certains composants. La prestation de ce dernier, d'un montant de 2,5 M€, semble surfacturée. Le sous-traitant reverse 17% du montant facturé (soit 425 k€) sur le compte d'une société commerciale immatriculée dans une place offshore asiatique. Cette société est gérée par un ressortissant du pays d'implantation du projet.

Critères d'alerte :

- Incohérence du circuit financier faisant intervenir une société asiatique pour une transaction sans rapport avec l'Asie.
- Le sous-traitant dans la fabrication de composants utilise des comptes bancaires différents pour d'une part percevoir les fonds du groupe industriel français, et d'autre part en transférer une partie vers la place offshore asiatique.
- Les 17% reversés à une société asiatique constituent un montant supérieur à la marge commerciale moyenne réalisée dans ce secteur d'activité. Ceci induit un soupçon de surfacturation.
- Le ressortissant qui gère la société asiatique destinataire des fonds a un profil de lobbyiste présent sur des secteurs d'activité variés, et non celui d'un spécialiste technique à même de fournir une prestation réelle en matière industrielle pour le projet concerné.



LES MANQUEMENTS AU DEVOIR DE PROBITÉ DE LA PART DE PERSONNES EXERÇANT UNE FONCTION PUBLIQUE

Plus encore que pour la corruption à l'international, les capteurs de Tracfin font du Service un acteur efficace dans la lutte contre les manquements au devoir de probité sur le territoire français, commis par des personnes exerçant une fonction publique. Tracfin caractérise de nombreux cas de corruption, de trafic d'influence, de prise illégale d'intérêts, de favoritisme ou de détournement de biens.

A ces infractions s'ajoute l'abus de confiance. De nombreux dossiers concernent des associations, de toutes tailles, souvent financées en tout ou partie sur fonds publics. A ce titre, le cadre juridique des associations, particulièrement souple en droit français, constitue une importante poche de risque dans le dispositif LCB/FT.

Prise illégale d'intérêts de la part d'un élu local

Cas n°25

L'adjoint au maire d'une ville moyenne est en charge de l'action sociale et des personnes âgées. Alors que la ville développe un projet de construction d'une maison de retraite, cet élu reçoit, en trois mois, 1 M€ viré sur le compte d'une SAS de conseil, et 0,6 M€ sur le compte d'une SAS immobilière, dont il est actionnaire.

Les fonds ont été versés par un promoteur et gestionnaire d'EHPAD, d'une part par le biais d'une SCI intermédiaire, d'autre part directement vers la SAS immobilière.

L'élu justifie ces arrivées de fonds par des factures établissant qu'il a produit une mission d'assistance et de conseil incluant la recherche du terrain, la mise en relation du promoteur et des propriétaires, l'assistance à la conception du projet, et la réalisation du dossier administratif.

Critères d'alerte :

- Fonctions de l'adjoint au maire
- Ouverture des deux SAS et fonctionnement de leurs comptes bancaires. L'arrivée rapide de ces virements importants, justifiés par des contrats d'apporteur d'affaires, constitue quasiment la seule activité des comptes.
- Liens personnels entre l'adjoint au maire et l'un des associés de la SCI intermédiaire ayant alimenté le compte de la SAS de conseil.
- L'élu a utilisé une partie des fonds pour se constituer un portefeuille d'assurance-vie, et investir dans un achat immobilier à titre privé.

Abus de confiance au détriment d'associations financées par subventions publiques

Cas n°26

Monsieur X est élu municipal d'une petite commune littorale. Son épouse dirige l'association de promotion de la foire du port de cette commune. Lui-même préside le comité d'organisation d'une importante fête foraine, qui se tient annuellement dans une ville moyenne de la région. En parallèle, le couple X dirige plusieurs autres associations, ayant par exemple pour objet l'aide aux forains retraités.

Les principaux clients des foires organisées sous la direction du couple X sont les Comités d'Œuvres Sociales des collectivités locales de la région (COS), ainsi que quelques comités d'entreprise. Ces entités achètent en gros les tickets d'entrée donnant accès aux attractions et manèges, pour les distribuer à leurs bénéficiaires (personnel des communes concernées, salariés et habitants).

Il apparaît qu'une partie des bénéfices des activités lucratives de vente de tickets sont détournés sur les comptes bancaires des associations dirigées par le couple X, voire directement sur ses comptes personnels ou ceux de SCI qu'il possède. Ces différents comptes bancaires font apparaître de fréquentes opérations suspectes, sous forme notamment de dépôts d'espèces.

Sur une période de trois ans, deux associations dirigées par le couple X ont été créditées d'un total de 290 k€ par différents paiements émanant principalement des COS et des comités d'entreprise, sans lien avec les objets des dites associations. Les fonds ont été en partie redistribués vers les comptes privés du couple X ou de leur entourage.

Tracfin a constaté, sur l'ensemble de ces comptes, un total de 240 k€ de dépôts d'espèces non justifiés, dont 160 k€ directement sur les comptes privés du couple. Le reste est ventilé sur les comptes de proches ou d'associations. Le couple mène un train de vie sensiblement supérieur à celui qui correspondrait à ses revenus déclarés, ses comptes bancaires affichant notamment des voyages d'agrément et l'achat de voitures de luxe.

Cas n°27

Monsieur Y est directeur territorial d'une métropole régionale et dirige, à ce titre, les services sociaux de la ville, incluant le Centre communal d'action social (CCAS). Parallèlement, il gère deux associations d'insertion professionnelle, entièrement financées par le CCAS. Il est également associé à Monsieur Z dans une société de distribution alimentaire. Monsieur Z, pour sa part, apparaît dans l'organigramme de trois autres associations d'insertion et de formation professionnelle, sur les comptes desquelles Monsieur Y a procuration.

En l'espace de deux ans, les diverses associations d'insertion professionnelle dirigées par Monsieur Y et Monsieur Z ont perçu près de 260 k€ de fonds publics, principalement en application de conventions passées avec le Centre Communal d'Action Sociale de la ville.

L'utilisation de ces fonds semble cependant peu conforme à l'objet des associations, puisqu'ils ont majoritairement fait l'objet de retraits en espèces, de prélèvements PayPal ou encore d'émissions de quelques chèques au profit de Monsieur Y.

Cas n°28

Une association d'insertion héberge des personnes en difficulté dans trois centres d'accueil. En l'espace de trois ans, elle a perçu un total de 4 M€ d'aides publiques, principalement apportées par le Conseil régional. Or, les comptes de l'association font apparaître sur la même période plusieurs anomalies :

- 470 k€ de retraits d'espèces, sans destination établie des fonds ;
- 225 k€ virés vers une SCI détenue par le président et la trésorière de l'association, dont 120 k€ virés du compte de la SCI vers le compte privé des parents du président ;
- de nombreux chèques et virements et chèques émis par l'association d'insertion au profit d'autres associations, actives dans la formation continue ou la gestion de centres de vacances, et dans l'organigramme desquelles le président, la trésorière ou leurs proches apparaissent.

LUTTE CONTRE LA FRAUDE FISCALE : TRACFIN GAGNE EN TECHNICITÉ ET RECUEILLE DES RENSEIGNEMENTS DÉTERMINANTS POUR LA DGFIP

En 2016, Tracfin a transmis 350 dossiers à l'administration fiscale. Ceux-ci concernent à 85 % des personnes physiques sur leur patrimoine privé (minoration de l'ISF, des droits de succession ou des droits de mutation), ou des dossiers reposant sur des flux non justifiés entre une personne morale et son dirigeant. Les 15% de dossiers concernant strictement des personnes morales pour des infractions fiscales portent principalement sur des fraudes à la TVA.[1]

Les déclarations de soupçon sur les particuliers couvrent un large spectre de fraudes. Les sujets les plus fréquemment déclarés traitent de la détention de comptes à l'étranger dans des pays frontaliers ou à fiscalité privilégiée, d'activités professionnelles non déclarées, d'organisation frauduleuse d'insolvabilité, ou d'abus de droit : exonération de plus-values, donations déguisées…

L'enjeu financier moyen par dossier tend à augmenter, de 1,33 M€ en 2015 à 1,41 M€ en 2016. Tracfin s'est concentré sur des dossiers à fort enjeu, impliquant souvent des ramifications internationales nécessitant des délais de traitement accrus.

Cependant, pour mieux valoriser les déclarations de soupçon portant sur des enjeux financiers plus modestes, Tracfin a mis en place au 2ème trimestre 2017 un processus de traitement accéléré des dossiers simples transmis à la DGFiP dit « Flash fiscaux ».

LES AVOIRS NON DÉCLARÉS À L'ÉTRANGER

Grâce à la coopération internationale entre CRF, Tracfin dispose de capacités de détection des comptes non déclarés à l'étranger qui sont particulièrement utiles à l'administration fiscale. Cette dernière va bénéficier, à partir de 2017, de la mise en place de l'échange automatique d'informations à caractère fiscale entre tous les pays signataires de la norme OCDE[2].

Le cas des trusts et les règles d'imposition qui leur sont applicables

La loi n°2011-900 du 29 juillet 2011 de finances rectificatives pour 2011 a institué en droit français un régime fiscal précis applicable aux trusts détenus à l'étranger. Les informations reçues par Tracfin témoignent que certains constituants ou bénéficiaires de trusts tentent encore de contourner ces dispositions, ou de ne les appliquer que partiellement.

Cas n°29

Monsieur Y était résident fiscal français de 2002 à 2014. Sur cette période, il n'a déclaré aucun avoir ni revenus d'avoirs à l'étranger, ainsi qu'un montant faible d'actif imposable à l'ISF. Lui et son épouse ont deux enfants, qui sont restés résidents fiscaux français après 2014.

Les renseignements collectés par Tracfin font état de la détention par Monsieur Y :

- D'un trust domicilié dans les îles anglo-normandes, dont lui et ses enfants sont bénéficiaires, et dont le montant des avoirs est de 35 M€. Ce trust verse chaque année aux membres de la famille bénéficiaires des distributions de plusieurs centaines de milliers d'euros.
- De nombreux comptes bancaires à l'étranger (Amérique du Nord, Union Européenne, îles anglo-normandes).
- Peu avant de changer de résidence fiscale, Monsieur Y et son épouse ont cédé les parts qu'ils détenaient dans une société de droit français, pour une valeur de 100 M€. Ils ont logé le produit de cette vente sur des comptes bancaires ouverts dans plusieurs pays de l'Union Européenne.

Ce faisant, Monsieur Y contrevient à plusieurs dispositions fiscales.

- Comptes bancaires à l'étranger :

En application des dispositions de l'article 1649 A du Code Général des Impôts (CGI), les comptes ouverts, utilisés ou clos, doivent être déclarés en même temps que les

1 Par ailleurs, des infractions fiscales sont mentionnées dans la majorité des dossiers judiciaires transmis aux Parquets. Elles apparaissent alors en marge d'autres infractions primaires telles que le travail dissimulé, l'escroquerie, l'abus de bien social ou les manquements à la probité.

2 Norme Commune de Déclaration (NCD/CRS) développée à la demande des dirigeants du G20 et approuvée par le Conseil de l'OCDE le 15 juillet 2014.

déclarations de revenus. Le défaut de production de cette déclaration entraîne l'application d'une amende fiscale ainsi que l'imposition de ces sommes.

• Omission déclarative de revenus de capitaux mobiliers :

En application des dispositions du 9° de l'article 120 du CGI, les produits distribués par un trust défini à l'article 792-0 bis, quelle que soit la consistance des biens ou droits placés dans le trust, sont considérés comme des revenus taxables.

De plus, l'article 123bis du CGI précise que lorsqu'un résident fiscal français possède au moins 10% des droits dans une fiducie ou équivalent établie à l'étranger, et que les actifs de cette entité juridique sont constitués de comptes courants ou de valeurs mobilières, les bénéfices produits par cette entité juridique constituent pour la personne physique concernée un revenu de capitaux mobilier[1].

• Dépôt de déclarations rectificatives de trust :

Monsieur Y a quitté le territoire français fin 2014. En 2015, il a déposé ses déclarations de constitution de trust et de valeur vénale annuelle au titre des années 2012 à 2014, en utilisant les modèles 2181-TRUST1 et 2181-TRUST2. Il précise que le trust aurait cessé d'avoir des liens de rattachement avec la France à la fin de l'année 2014, et ne dépose donc aucune déclaration au titre de 2015. En effet, les enfants de Monsieur Y ont émis fin 2014 des déclarations de renonciations temporaires.

L'article 1649 AB du CGI dispose que l'administrateur d'un trust dont le constituant ou l'un au moins des bénéficiaires a son domicile fiscale en France, ou qui comprend un bien ou un droit qui y est situé, doit en déclarer la constitution, la modification ou l'extinction ainsi que le contenu de ses termes.

Depuis fin 2014 Monsieur Y est non résident. Toutefois, ses deux enfants bénéficiaires du trust sont toujours résidents fiscaux français. Ainsi, un renoncement temporaire au bénéfice du trust pourrait avoir pour objet de s'exonérer de cette obligation déclarative. Ce renoncement temporaire pourrait n'avoir qu'un but fiscal.

• Minoration d'ISF :

Depuis 2012, en application des dispositions de l'article 885 G ter du CGI, les biens placés dans un trust, y compris les produits capitalisés, sont inclus dans le patrimoine taxable à l'ISF du constituant.

• Omission déclarative d'exit tax :

L'article 167 bis du CGI prévoit, entre autres, que le transfert de domicile fiscal hors de France entraîne l'imposition immédiate à l'impôt sur le revenu et aux prélèvements sociaux des plus-values latentes sur les titres, sous condition tenant à l'importance des participations détenues, des créances trouvant leur origine dans une clause de complément de prix, et de certaines plus-values en report d'imposition.

Or Monsieur et Madame Y n'ont pas déposé de déclaration en ce sens. Pourtant, lorsqu'ils ont cédé les parts qu'ils détenaient dans une société française pour 100 M€, la convention de cession de titres précisait que le prix pourrait être ultérieurement augmenté en fonction de certains critères définis entre les parties. Le montant éventuel d'un complément de prix ainsi défini aurait dû être mentionné dans le cadre de la déclaration d'*exit tax*.

1 Art. 123 bis du CGI : « 1. Lorsqu'une personne physique domiciliée en France détient directement ou indirectement 10 % au moins des actions, parts, droits financiers ou droits de vote dans une entité juridique - personne morale, organisme, fiducie ou institution comparable - établie ou constituée hors de France et soumise à un régime fiscal privilégié, les bénéfices ou les revenus positifs de cette entité juridique sont réputés constituer un revenu de capitaux mobiliers de cette personne physique [...] lorsque l'actif ou les biens de la personne morale [...] sont principalement constitués de valeurs mobilières, de créances, de dépôts ou de comptes courants. »

Le crédit lombard, instrument de rapatriement d'avoirs non déclarés

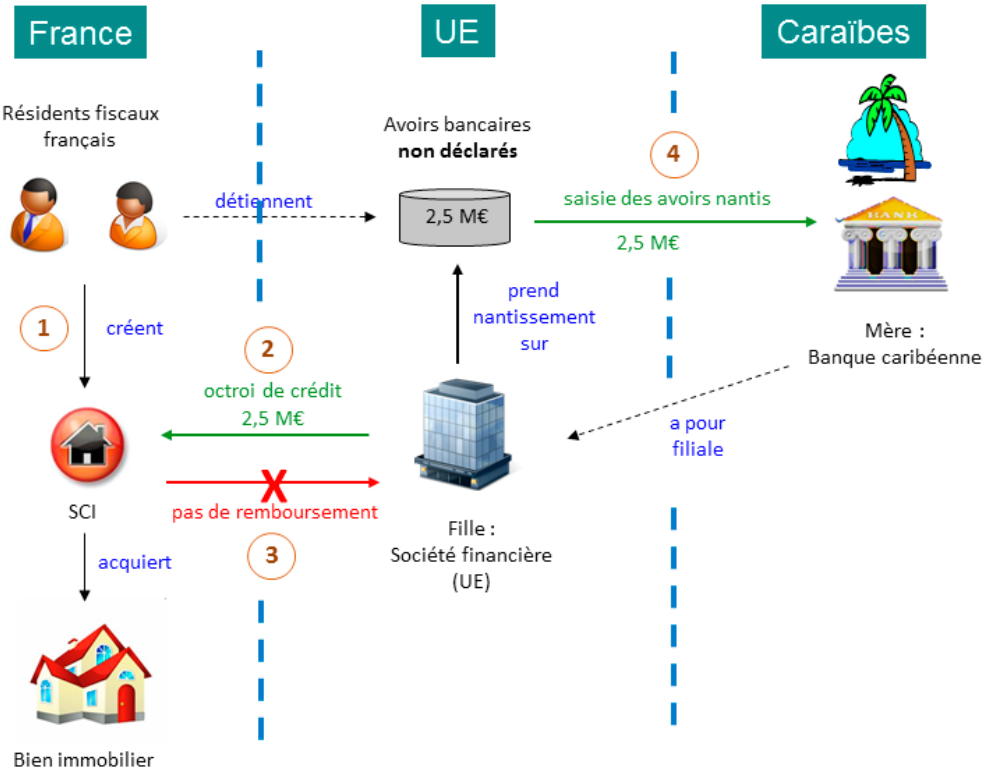
L'utilisation du crédit lombard gagé sur des avoirs non déclarés, afin de rapatrier ceux-ci, est une technique de blanchiment de fraude fiscale connue et toujours pratiquée.

Cas n°30

Un couple de résidents fiscaux français crée une SCI afin de procéder à un achat immobilier. Pour financer l'acquisition, la SCI emprunte 2,5 M€ à une société financière immatriculée dans l'Union Européenne, filiale d'une discrète banque caribéenne. Le crédit est dit « lombard » ou « back-to-back », en ce sens qu'il est nanti sur des valeurs mobilières, détenues sur un compte d'une autre banque européenne, mais non déclarées à l'administration fiscale française.

Au bout d'un an, la banque caribéenne constate le non-paiement des mensualités de remboursement du crédit, le place en défaut, et fait saisir les valeurs mobilières objet du nantissement. Pour prix de ces services, la banque facture à la famille bénéficiaire une commission de 3 % du montant du crédit décaissé.

Le crédit-lombard a permis *in fine* à la famille bénéficiaire de rapatrier en franchise d'impôts des avoirs étrangers non déclarés à hauteur de 2,5 M€.



LES ABUS DE DROIT : DÉTOURNEMENT DU PEA ; DONATIONS AVANT CESSION

L'utilisation abusive du PEA afin de convertir une rémunération imposable en plus-value exonérée

Le Plan d'Épargne en Actions (PEA) permet à un résident fiscal français d'acquérir un portefeuille d'actions d'entreprises européennes tout en bénéficiant, sous conditions, d'une exonération d'impôt sur les plus-values réalisées sur ces titres. Ce cadre légal est fréquemment détourné par certains contribuables qui ne respectent pas les conditions restrictives donnant droit à l'exonération.

Ils acquièrent auprès de leur employeur des actions de leur société à un prix très préférentiel, placent ces titres dans un PEA, puis les revendent à l'employeur au bout de quelques mois à un prix multiplié par 20 ou 30. Il s'agit de déguiser une rémunération en opération d'achat/revente de titres, exonérée d'imposition sur la plus-value, ce que la jurisprudence caractérise comme un abus de droit.

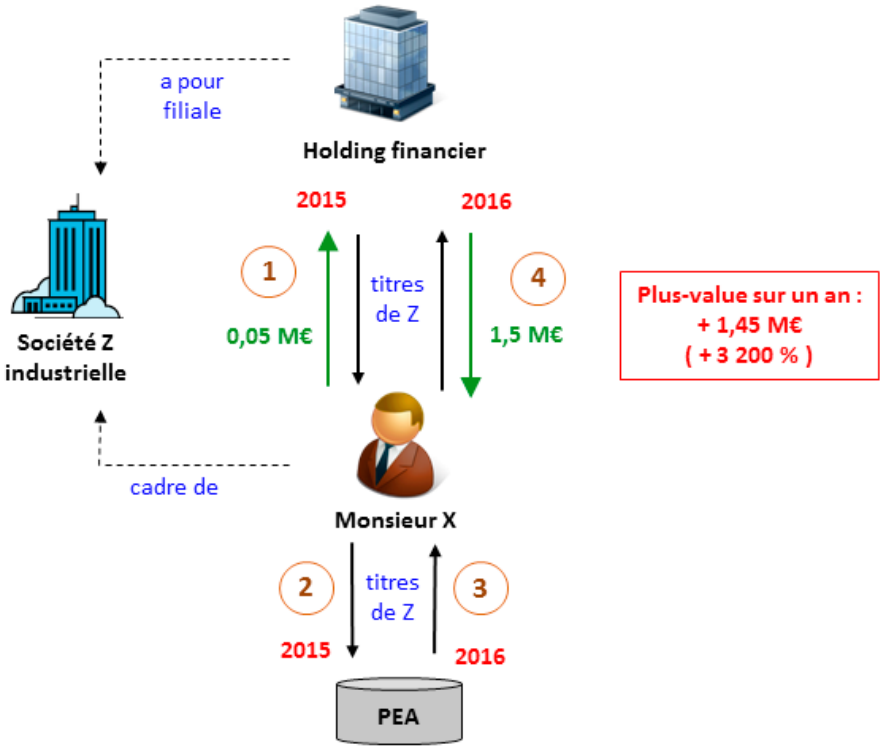
Cas n°31

La société italienne Z, active dans la fabrication de composants industriels, est non cotée et détenue par une holding étrangère. Monsieur X, cadre d'une filiale française de la société Z, achète à la holding étrangère 10 titres de la société Z pour 45 k€, les place dans son PEA, puis les revend 12 mois après à cette même holding pour 1,5 M€.

Monsieur X présente la plus-value dégagée comme exonérée d'imposition, car réalisée dans le cadre de son PEA. Or, le déroulement de l'opération laisse présumer l'existence d'une fraude :

- Acquisition des titres objet de l'opération par les membres de la direction de la filiale française.
- Opérations d'achat/revente de titres réalisées entre les mêmes parties, le vendeur initial des titres étant aussi l'acquéreur final.
- Augmentation de la valeur des titres de 3200 % sur 12 mois alors que le chiffre d'affaires de la société Z est en nette baisse, et le résultat stable.

Cette opération s'analyse comme une rémunération déguisée en franchise d'impôts, par l'utilisation du cadre légal privilégié du PEA. La jurisprudence considère comme abusive le fait de transférer dans un PEA une rémunération déguisée, et l'administration peut remettre en cause l'opération au travers de l'abus de droit, prévu à l'article L64 du Livre des procédures fiscales.



Ce type d'abus est également constaté dans le cadre des opérations de *Leverage Buy Out* (LBO), ou rachat de société avec effet de levier. Un fonds d'investissement propose de racheter une société en associant les dirigeants de la cible à l'opération en capital. L'acquisition est principalement financée par endettement, logé dans le bilan de la cible. Celle-ci devra rembourser sa dette en améliorant ses capacités opérationnelles afin de dégager des *cash flows* suffisants. A la fin du processus, les acheteurs sont en possession d'une société sensiblement désendettée et nettement mieux valorisée, qu'ils vont chercher à revendre ou à introduire en bourse. La faible part de capitaux propres que les acheteurs avaient investie initialement voit sa valeur démultipliée.

Les dirigeants de la société cible qui avaient investi dans l'opération peuvent être tentés de placer dans un PEA les titres de la cible qu'ils avaient acquis, afin de bénéficier de l'exonération de plus-value.

Cas n°32

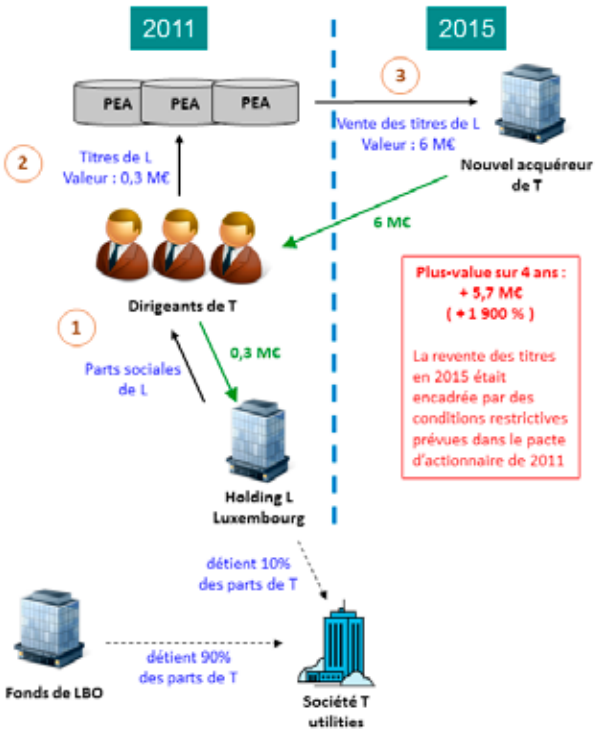
La société T, active dans les services aux collectivités, a fait l'objet de deux opérations successives de *Leverage Buy Out* en 2011 et 2015, associant à chaque fois un fonds d'investissement et les dirigeants de l'entreprise. Pour ces opérations en capital, les dirigeants personnes physiques sont intervenus à partir du holding luxembourgeois L, dans lequel ils se sont regroupés pour porter les parts de la société T.

Les dirigeants salariés de T ont réalisé au sein de leur PEA des opérations d'achat/revente de titres du holding L. Les titres, achetés 300 k€ en 2011, ont été revendus pour 6 M€ en 2015, soit une plus-value de 1 900 % en 4 ans. La plus-value dégagée a été investie en assurance-vie.

Or, les conditions d'acquisition et de cession des titres de la société L ne semblent pas s'inscrire dans le cadre d'un libre échange, tant au regard du prix d'achat que des conditions restrictives de cession de titres.

Ces opérations semblent avoir pour objectif de rémunérer les membres de la direction du groupe, en franchise d'impôts, par l'utilisation abusive du cadre légal privilégié du PEA.

Le Conseil d'Etat, en septembre 2014, a précisé que lorsque les titres sont attribués dans des conditions préférentielles octroyées eu égard à la qualité de salarié ou de mandataire social, sans aucune prise de risque financier, ou en contrepartie d'un investissement modique, les gains qui en sont issus constituent un avantage en argent imposable dans la catégorie des traitements et salaires[1].



1 Décision du Conseil d'Etat n°365573 du 26 septembre 2014

La technique des donations avant cession

La pratique des donations avant cession est devenue une technique d'optimisation fiscale qui permet de purger des plus-values latentes. Toutefois, cette opération peut être remise en cause dans le cadre de l'abus de droit prévu à l'article L64 du Livre des procédures fiscales (LPF)[1].

La jurisprudence du Conseil d'État remet en cause avec constance les donations pour lesquelles il y a réappropriation d'une partie des produits de la cession par le donateur.

Cas n°33

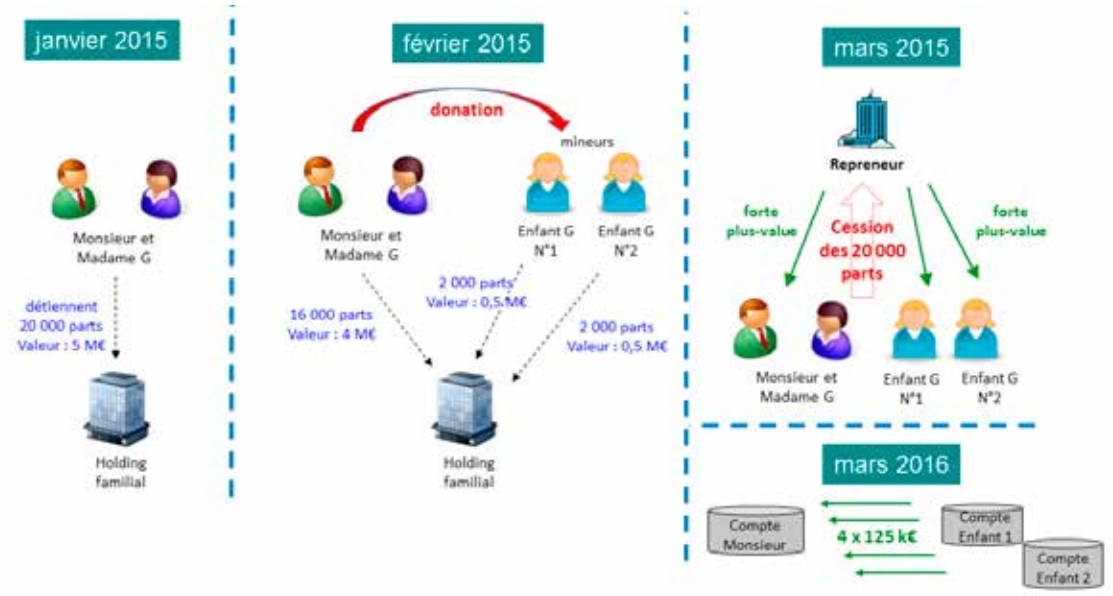
Monsieur et Madame G possèdent 20 000 parts sociales d'une holding familiale, d'une valeur nominale unitaire de 250 €, soit un patrimoine de 5 M€.

Ils donnent à chacun de leurs deux enfants mineurs 2 000 parts sociales de cette holding, soit une donation d'une valeur de 500 k€ à chaque enfant. Monsieur et Madame G conservent pour eux 16 000 parts. Sur cette donation, un abattement total de 200 k€ a été appliqué, conformément à l'article 779 I du code général des impôts (CGI).

Un mois plus tard, tous les membres de la famille G cèdent leurs parts à une société tierce, toujours à la valeur unitaire de 250 €. La cession des parts de Monsieur et Madame G permet la réalisation d'importantes plus-values. Celles-ci font l'objet d'un abattement pour durée de détention. Ils déposent comme il se doit les déclarations n°2074 relatives au calcul des plus-values.

Un an plus tard, Monsieur G crédite son compte bancaire de quatre virements d'environ 125 k€ chacun, en provenance des comptes de ses deux enfants. Ainsi Monsieur G semble se réapproprier les fonds perçus par ses enfants mineurs lors des opérations de cession des parts intervenues un an auparavant.

La jurisprudence du comité consultatif pour la répression des abus de droit établit qu'une opération de donation-cession peut être critiquée si la donation n'est pas réelle et n'entraîne pas une dépossession définitive de l'auteur. Au cas d'espèces, la remise en cause de la donation avant cession a pour conséquence de rendre immédiatement imposable la plus-value sur la quote-part des titres objet de la donation aux enfants, cette dernière ayant bénéficié d'un abattement de 200 k€.



1 Art. L64 du LPF : « L'administration est en droit d'écarter comme ne lui étant pas opposables les actes constitutifs d'un abus de droit, soit que ces actes ont un caractère fictif, soit que, recherchant le bénéfice d'une application littérale des textes ou de décisions à l'encontre des objectifs poursuivis par leurs auteurs, ils n'ont pu être inspirés par aucun autre motif que celui d'éluder ou d'atténuer les charges fiscales que l'intéressé, si ces actes n'avaient pas été passés ou réalisés, aurait normalement supporté eu égard à sa situation réelle ou à ses activités réelles. »

LA FRAUDE SOCIALE, COMBATTUE PAR UNE COOPÉRATION RENFORCÉE ENTRE SERVICES, ÉVOLUE AVEC LES TRANSFORMATIONS DE L'ÉCONOMIE

Tracfin développe une action résolue contre les fraudes sociales. L'article 129 de la loi n°211-1906 du 21 décembre 2011 de financement de la sécurité sociale pour 2012 inclut les organismes de protection sociale parmi les destinataires des transmissions de Tracfin. Le 1er mars 2012, Tracfin a signé un protocole avec les principaux organismes de protection sociale afin de développer un partenariat étroit : ACOSS (URSSAF), CNAMTS, CNAVTS, CCMSA, CNAF, Pôle Emploi, RSI.

En 2016, 165 dossiers ont été transmis à ces organismes, soit une hausse de + 51 % par rapport à 2015. Le nombre de droits de communication envoyés par Tracfin à ces organismes a augmenté dans les mêmes proportions. Les enjeux financiers totaux s'élèvent à 140 M€. L'ACOSS est le principal destinataire. Le secteur du BTP est de loin le plus représenté, du fait de la prépondérance des déclarations de soupçon portant sur l'emploi de main d'œuvre non déclarée.

Les principales typologies de fraude sociale rencontrées par Tracfin varient peu :

- Fraudes aux cotisations non versées :
  - Travail dissimulé et emploi de main d'œuvre non déclarée.
  - Minoration de l'assiette des cotisations sociales par dissimulation d'une partie de l'activité.
- Fraudes aux prestations indûment perçues :
  - Activité professionnelle non déclarée parallèlement à la perception d'allocations.
  - Fraude à la résidence en France.
  - Détournement de prestations de retraite dans un schéma de comptes collecteurs.
  - Fraude des professionnels de santé et fraudes aux mutuelles complémentaires.

LES COMPTES COLLECTEURS DE PENSIONS DE RETRAITE : UNE ACTION RÉSOLUE SUR LE LONG TERME

La problématique des comptes collecteurs de pensions de retraite a fait l'objet depuis 2013 d'une action concertée de la Délégation Nationale à la Lutte contre la Fraude (DLNF), de la Caisse Nationale d'Assurance Vieillesse (CNAV) et de Tracfin. Le nombre de cas constatés est en baisse, même si le risque reste élevé. Au total, les 31 dossiers transmis par Tracfin entre 2013 et 2016 ont permis à la CNAV de diligenter plusieurs centaines de contrôles de dossiers individuels. Environ 15% des dossiers de non-résidents contrôlés se sont révélés frauduleux. Ce type de fraude constitue toujours un risque élevé, le principal dossier transmis en 2016 portant sur des enjeux financiers importants.

Les personnes ayant travaillé en France perçoivent à ce titre des prestations sociales, notamment des prestations de retraite de la CNAV, qu'elles soient résidentes ou non sur le territoire français. Les prestations sont versées sur les comptes bancaires français des ayant droits.

Dans le cas des bénéficiaires non-résidents, la fraude consiste à ne pas déclarer le décès de l'assuré bénéficiaire, afin que des tiers continuent de toucher les prestations. Celles-ci sont transférées, par virements ou transferts d'espèces, des comptes français des pensionnés vers un nombre restreint de comptes centralisateurs. Les fonds sont ensuite virés à l'étranger, principalement vers le Maghreb.

Tracfin a identifié des comptes de collecte alimentés par des dizaines, parfois des centaines de comptes de pensionnés, et recensé des intermédiaires mandataires, dits « collecteurs ». Les flux financiers retracés démontrent le détournement des versements. Des cas de fraude documentaire ont été relevés dans les documents d'identité utilisés pour l'ouverture des comptes ou les demandes de mandat, et corroborés avec les éléments de la CNAV.

Certains collecteurs se trouvent être des intermédiaires au sein d'organisations pyramidales plus vastes. Ils sont alors eux-mêmes objets de collectes vers des niveaux supérieurs. Dans d'autres cas, la collecte est suivie d'achats en France de biens de consommation divers, destinés à être expédiés vers le Maghreb. Ce schéma implique la présence de sociétés d'import-export de taille significative et bien implantées en France.

Les critères d'alerte sont les suivants :

Pour la CNAV :

- caisses de retraite multiples alimentant une même agence ;
- proportion anormalement élevée de bénéficiaires très âgés ;
- contradiction dans les justificatifs reçus pour un même dossier : acte de décès envoyé par certains membres de la famille et attestation d'existence envoyée par des tiers ;
- l'assuré bénéficiaire n'est pas le titulaire du compte bancaire sur lequel est versée la pension.

Pour les établissements bancaires :

- le compte bancaire a été ouvert avec de faux documents ;
- présence sur le compte d'un mandataire, collecteur des sommes versées par les caisses de retraite ;
- mouvements de fonds : les prestations reçues font l'objet de retraits réguliers et importants en espèces, ou de transferts de fonds, en France ou à l'étranger.

Tandis que ce type de schéma parvient à être endigué par une coopération résolue et de long terme entre les organismes publics concernés, le développement de l'économie collaborative repose sous un nouveau jour le problème de la fraude aux cotisations sociales.

LA FRAUDE AUX COTISATIONS SOCIALES DANS LE CADRE DE L'ÉCONOMIE COLLABORATIVE

La montée en puissance de l'économie collaborative entraîne l'apparition d'un nouveau type de dossiers, en particulier dans le secteur des Voitures de Transport avec Chauffeurs (VTC). Certaines sociétés semblent faire une utilisation abusive du statut d'auto-entrepreneur afin de ne pas verser de charges sociales, alors qu'elles imposent à leurs chauffeurs un lien de subordination avéré.

Cas n°34

La société K a pour objet le transport public de personnes. Dès sa première année d'activité, ses comptes bancaires présentent un total de flux créditeurs de 2,5 M€, dont l'essentiel est constitué de virements en provenance d'une grande plate-forme de VTC.

Au débit, les flux sont constitués de virements et de chèques à destination de particuliers et de sociétés du secteur automobile (vente et location). Les particuliers bénéficiaires des flux ont fait l'objet de déclarations préalables à l'embauche (DPAE) par la société.

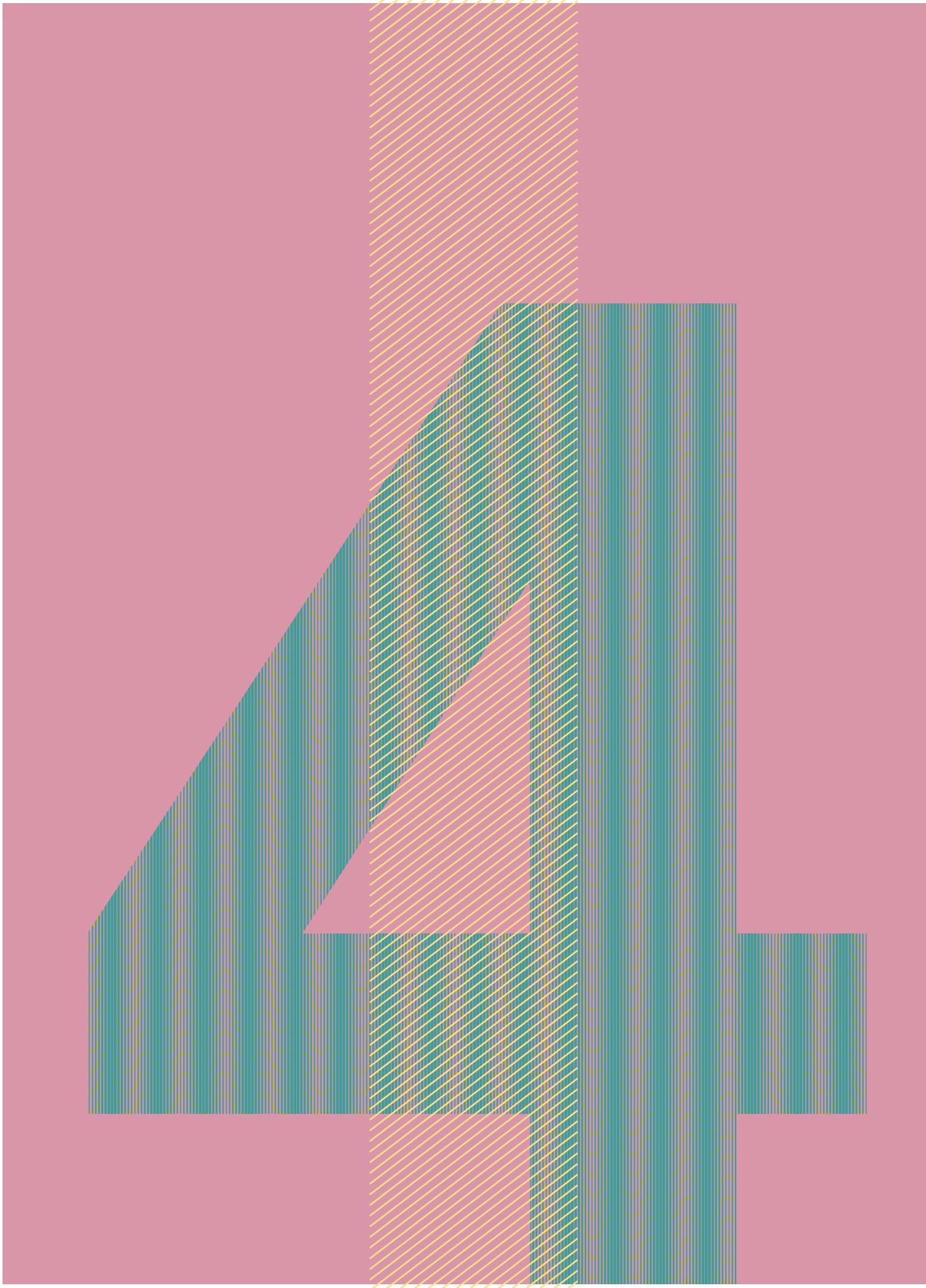
La société K déclare à l'URSSAF un total de salaires versés de 315 k€ pour 35 salariés, alors même qu'elle a mentionné 230 DPAE. Sur l'exercice suivant, elle présente des incohérences répétées entre les montants de salaires versés, relativement stables, et le nombre de salariés déclarés, très fluctuant.

Ces incohérences entre salaires déclarés et nombre de salariés s'expliquent par le recours à des chauffeurs ayant la qualité d'auto-entrepreneurs. A l'issue de leur période d'essai, la plupart des chauffeurs recrutés comme salariés optent finalement pour le statut d'auto-entrepreneurs. La société K aurait seulement une trentaine de salariés stables en moyenne sur l'année. L'essentiel des effectifs est constitué par un important *turn-over* de chauffeurs. La société ne procède pas par CDI ni CDD, mais par une DPAE qui ne se convertit pas à l'issue de la période d'essai.

Il s'avère qu'il y a abus de l'utilisation de la qualité d'auto-entrepreneur, dans la mesure où les chauffeurs restent liés par un lien de subordination avec la société K :

- Elle est leur seul employeur : les courses sont exclusivement fournies aux chauffeurs par la société.
- Elle leur met à disposition leur matériel de travail qu'est le véhicule. La société K dispose d'au moins une cinquantaine de véhicules identifiés, en partie achetés sur son patrimoine propre, en partie loués en leasing. Le lien de subordination est également conforté par l'organisation de la fixation des tarifs, et par les instructions que celles-ci leur donne pour l'exercice de l'activité.
- Elle impose les conditions tarifaires et fixe des instructions pour l'exercice de l'activité.

Ainsi, la société K ne déclare aux URSSAF qu'une trentaine de salariés, pour un effectif réel moyen d'au moins cinquante chauffeurs, ceci afin de ne pas payer les charges sociales sur une grande partie de ses employés.



LA RÉVOLUTION TECHNOLOGIQUE EN COURS DANS LES SERVICES FINANCIERS PORTE EN GERME UN BOULEVERSEMENT DU SECTEUR QUI APPELLE UNE ADAPTATION DE LA RÈGLEMENTATION LCB/FT

Les sociétés dites FinTech[1] utilisent les innovations technologiques de la révolution numérique pour proposer des services financiers simples d'utilisation, rapides et moins chers. L'offre s'est développée en priorité dans les services de paiement et la gestion de comptes. L'émergence de nouveaux prestataires de services de paiement bouleverse le secteur bancaire traditionnel. L'évolution devrait s'accélérer avec l'arrivée sur ces activités des géants du Web ou des opérateurs de téléphonie mobile. La conjugaison de nouvelles solutions techniques limite l'efficacité des dispositifs LCB/FT existants en diluant les contrôles de conformité menés par les opérateurs agréés. La règlementation tente de s'adapter aux mutations du secteur, mais le mouvement n'en est qu'à ses débuts.

LA MULTIPLICATION DES NOUVEAUX PRESTATAIRES DE SERVICES DE PAIEMENT COMPLIQUE LA TRAÇABILITÉ DES FLUX FINANCIERS

LES ÉTABLISSEMENTS DE PAIEMENT ET DE MONNAIE ÉLECTRONIQUE SE MULTIPLIENT, CONFORTÉS PAR LES DIRECTIVES EUROPÉENNES

Les nouveaux prestataires de services de paiement (PSP) peuvent prendre plusieurs formes, dont :

– les plateformes numériques de gestion en ligne des paiements et des encaissements, qui s'apparentent à des infrastructures utilisables soit par d'autres prestataires de services de paiement, soit directement par les commerçants ou les clients finaux ;
– les autres prestataires (applications de services de paiement, plateformes de *crowdfunding*, émetteurs de cartes de paiement) qui viennent s'intercaler entre le client final et la plate-forme numérique de gestion des flux.

Les PSP proposent à leurs clients des portefeuilles de monnaie électronique (ou *wallets*) rechargeables à partir (i) de comptes bancaires, (ii) d'autres portefeuilles de monnaie électronique, voire (iii) à partir d'espèces via des supports physiques de type cartes prépayées ou tickets-coupons. Ces opérateurs interagissent entre eux via des API[2], qui permettent à leurs systèmes informatiques de dialoguer avec fluidité.

Ces acteurs profitent de la directive européenne sur les services de paiement de 2015, dite DSP2, qui a été transposée en droit français au mois d'août 2017[3]. Elle consacre les nouveaux acteurs issus des FinTech. Il s'agit en premier lieu des établissements de paiement et de monnaie électronique, ainsi que des agrégateurs de comptes et des initiateurs de paiement[4]. La DSP2 met fin à une forme de monopole bancaire sur les services de paiement, ce qui offre aux nouveaux prestataires de services de paiement une vaste marge de manœuvre commerciale.

1 FinTech est la contraction de *financial technologies*.

2 API : Application Programming Interface

3 Directive (UE) 2015/2366 du 25 novembre 2015, transposée en droit français par l'ordonnance n°2017-1252 du 9 août 2017, ainsi que les décrets et arrêtés liés (Cf Journal officiel des 10 août et 2 septembre 2017). La date limite de transposition de la DSP2 pour l'ensemble de l'UE est fixée au 13 janvier 2018.

4 PSIC (Prestataires de Services d'Informations sur les Comptes) et PSIP (Prestataires de Services d'Initiation de Paiement).

LA TRAÇABILITÉ DES FLUX FINANCIERS DEVIENT PLUS DIFFICILE À ÉTABLIR

L'émergence de ces opérateurs complique la traçabilité des flux financiers. Les PSP viennent s'interposer entre le client et sa banque. Le client enregistre les coordonnées de son compte ou de sa carte bancaire auprès d'un PSP, lequel gère les paiements vis-à-vis des tiers. De ce fait, le PSP prive la banque d'une partie des données nécessaires à l'analyse fine des opérations du client. La banque ne voit plus que le PSP comme seule contrepartie des flux du compte de son client.

Pour exercer leur activité, les PSP doivent être agréés auprès d'un superviseur bancaire, qui leur impose des mesures de vigilance LCB/FT. En droit français, ils peuvent notamment choisir le statut d'établissement de paiement (EP) ou d'établissement de monnaie électronique (EME), délivré par l'Autorité de Contrôle Prudentiel et de Résolution (ACPR)[1]. Selon l'article L.561-2 du code monétaire et financier, les EP et les EME sont assujettis au dispositif LCB/FT, qui leur impose des obligations de vigilance client[2] et des obligations déclaratives envers Tracfin.

Le dispositif LCB/FT reste cependant fragile, compte-tenu de son périmètre d'application fonctionnel et géographique.

Sur le plan fonctionnel, un dispositif efficace doit couvrir tous les acteurs pertinents. La réglementation LCB/FT devrait cibler les acteurs détenant la meilleure connaissance du client final. Or, les établissements financiers agréés (banques, EP, EME) détiennent parfois moins de données clients que d'autres acteurs de plus en plus actifs sur le secteur des paiements, tels que les grands acteurs du web 2.0 ou les opérateurs de téléphonie mobile. Ceux-ci, à ce jour, ne sont pas en tant que tels assujettis au dispositif LCB/FT[3].

Sous l'angle géographique, les exigences en matière LCB/FT doivent être homogènes entre pays. Or, tous les pays n'ont pas le même degré d'exigence, tant concernant les modalités d'attribution d'un agrément que le contrôle des opérateurs. Au sein même de l'Espace Economique Européen, le régime de la libre prestation de services (LPS) permis par le passeport européen restreint le pouvoir de contrôle des superviseurs nationaux (cf infra partie 5.). Les distorsions entre pays limitent l'efficacité du dispositif LCB/FT. Le renforcement des coopérations risque d'être insuffisant sans harmonisation substantielle des modalités concrètes d'agrément et de contrôle.

1 Les acteurs du *crowdfunding* relèvent du statut d'intermédiaire en financement participatif (IFP) ou de celui de conseiller en investissement participatif (CIP).

2 Identifier et vérifier l'identité de leur client (art. L.561-5 du CMF) ; caractériser la relation d'affaire (art. L.561-5-1 du CMF) ; contrôler la cohérence des opérations client pendant toute la durée de la relation (art. L.561-6 du CMF).

3 Seule une filiale dédiée ou, le cas échéant, une société partenaire, aura le statut d'établissement de crédit, de paiement ou de monnaie électronique, et sera donc assujettie au dispositif LCB/FT. Le grand groupe lui-même restera en-dehors du périmètre.

LES GRANDS ACTEURS DE L'INTERNET SONT À L'OFFENSIVE DANS LES SECTEURS DU TRANSFERT DE FONDS ET DU PAIEMENT MOBILE

UN AVANTAGE DÉCISIF : LA MAÎTRISE DES DONNÉES DE MASSE

Les grands acteurs du Web qui ont impulsé la révolution digitale et acquis des positions dominantes imposent de nouveaux modèles économiques basés sur l'exploitation de données. Conjuguant puissance financière et adhésion massive des consommateurs, ils disposent d'une force de frappe inédite pour investir la sphère des services financiers. Ils pourraient remodeler de manière significative le secteur des services de paiement.

Leur maîtrise technique et leur expertise en matière de collecte et d'analyse de données de masse leur permettent de concurrencer les banques sur plusieurs métiers historiques comme les moyens de paiement ou les offres de crédit. Leur capacité à tracer et anticiper le parcours d'achat en ligne d'un consommateur peut les amener à se substituer aux acteurs bancaires pour certains produits et services, grâce à une meilleure connaissance client.

Les grands acteurs de l'internet sont eux-mêmes irrigués par de nombreuses start-up. Ils profitent des innovations de celles-ci tout en leur offrant des perspectives de développement immédiates, dans une alliance de services particulièrement efficace.

Des solutions déjà développées et disponibles concernent les services de transferts de fonds internationaux, les services de paiement instantané par internet et par téléphone mobile, ainsi que les prêts aux entreprises.

LA CHINE EST UN MARCHÉ PRÉCURSEUR

La Chine fait figure de précurseur dans la révolution digitale des services de paiement. Les leaders chinois du e-commerce, de la téléphonie et du web 2.0 ont commencé leur conquête du secteur financier il y a une dizaine d'années, inspirant fortement leurs homologues occidentaux. Cette supériorité s'explique notamment par le poids de la Chine en matière de e-commerce au niveau mondial (672 Md$ en 2016, soit 40% du e-commerce mondial, qui devrait atteindre 1 600 Md$ en 2018), un réservoir d'utilisateurs considérable (certains réseaux sociaux chinois rassemblent jusqu'à 550 millions d'utilisateurs) et un système bancaire local éprouvant des difficultés à s'adapter aux transformations digitales de l'économie. Les leaders du Web chinois proposent une offre large qui couvre l'ensemble des services bancaires : système de paiement, portefeuille électronique, banque en ligne, placement d'épargne.

Forts de leur hégémonie locale, certains de ces acteurs tendent à s'exporter hors de Chine pour s'implanter en Asie du Sud-Est mais également en Europe. En 2016, un de ces géants chinois a conclu un partenariat avec une banque française pour proposer aux commerçants français une solution facilitant les paiements des touristes chinois. Destinée à une clientèle dépensière, la solution prend la forme d'un paiement mobile sans contact initié depuis un portefeuille de monnaie électronique détenu et alimenté par le consommateur chinois à partir de son compte bancaire en Chine. Il permet à l'utilisateur de dépenser jusqu'à 40 000 € en une seule transaction, qu'il est possible de répéter autant de fois que souhaité. Or, si un dispositif de conformité est exercé par la banque française partenaire, celui-ci ne porte que sur les commerçants bénéficiaires des fonds. Dès lors, la banque française ne possède aucune information sur le donneur d'ordre, l'origine des fonds, ni la méthode de chargement du compte utilisé. La vigilance BC/FT sur l'émetteur repose sur le service conformité de la société chinoise.

Des solutions relativement similaires sont développées par des acteurs occidentaux, tant dans le domaine du paiement mobile que du paiement instantané sur Internet. Ces services, lorsqu'ils sont conjugués à l'utilisation de cartes prépayées, participent à opacifier les flux financiers. Leur propagation auprès des utilisateurs peut s'avérer extrêmement rapide.

DES FERTILISATIONS CROISÉES ENTRE GRANDS ACTEURS DU NET ET START-UP

Le réservoir de consommateurs entretenus par certains acteurs du Web ouvre des opportunités de développement immédiates pour des start-ups innovantes.

Cas n°35

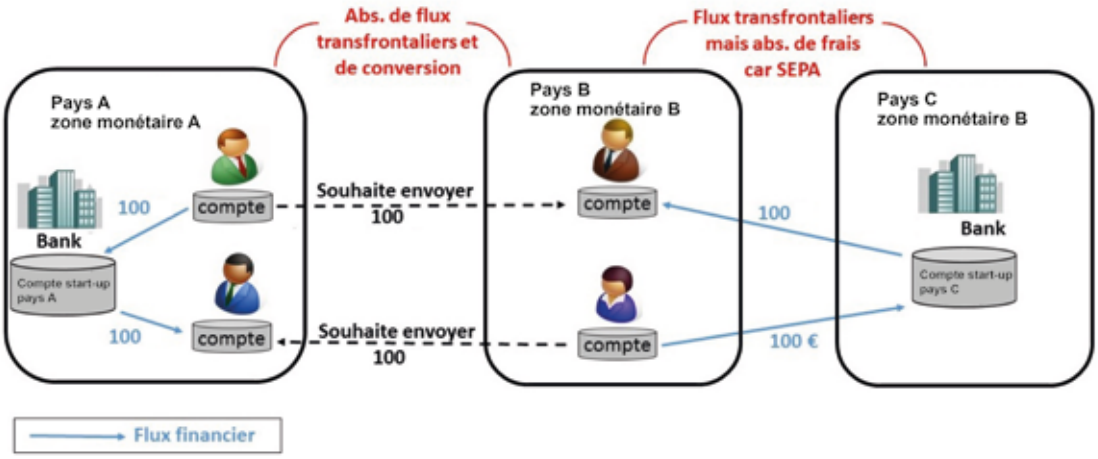
Une de ces start-up propose un service de transfert international de fonds avec conversion de devises, qui utilise le principe de la compensation pour éviter aux clients le coût des virements bancaires internationaux et des frais de change. Le mécanisme de la compensation, contraire aux principes comptables élémentaires, coupe la traçabilité d'un flux financier. Ceci impose à l'opérateur une responsabilité particulière afin de reconstituer cette traçabilité s'il veut remplir ses obligations LCB/FT.

De plus, cette start-up n'impose aucun plafond limitant le montant des transferts.

En France, la société opère grâce au passeport européen sous le régime de la Libre Prestation de Services. Elle n'a pas besoin d'avoir d'implantation sur le territoire national.

Les transactions étudiées par Tracfin concernent des flux depuis ou vers des pays occidentaux ou asiatiques développés, générés par une clientèle essentiellement expatriée ou retraitée, qui utilise ce service pour des rapatriements de fonds ou des investissements immobiliers. Mais l'utilisation de ses services donne lieu dans certains cas à des opérations douteuses, pour des montants conséquents.

Le succès de ce type d'offre attire les acteurs du Web 2.0. Un grand acteur du net permet depuis peu d'utiliser le service de transferts internationaux de fonds de cette start-up, à partir de la plateforme d'échange d'un réseau de discussion. La seule communication du nom, du prénom et de l'adresse e-mail du bénéficiaire suffisent aux utilisateurs du même réseau à ordonner un paiement. Aucune des sociétés parties prenantes de ce service n'étant immatriculée en France, les opérations demeurent difficilement traçables par Tracfin, sauf demande expresse auprès des CRF étrangères concernées.



LA PROMOTION DE L'ANONYMAT : LA SUPERPOSITION DE NOUVEAUX OUTILS CONJUGUANT MONNAIE ÉLECTRONIQUE, MONNAIE VIRTUELLE OU MATIÈRES PREMIÈRES

Tracfin constate des cas d'utilisation conjuguée de monnaie électronique et de monnaie virtuelle au sein d'une même opération : envoi de fonds conjointement sur des cartes prépayées et sur des plateformes d'échanges de monnaies virtuelles ; comptes de paiement utilisés comme supports d'opérations sur des plateformes de marché... La superposition des instruments de paiement est généralement le signe d'une volonté d'opacification. Or, les outils disponibles pour ce faire se multiplient.

LES *BLOCKCHAINS* SPÉCIFIQUEMENT DÉVELOPPÉES POUR L'ANONYMAT

La blockchain bitcoin, initialement perçue comme un puissant vecteur d'anonymat, n'offre en réalité qu'un anonymat partiel. Si la blockchain bitcoin est actuellement accessible sans procédure de connaissance client (KYC) et qu'il est possible d'ouvrir autant de portefeuilles que souhaité sans donner d'identité, une caractéristique essentielle de la blockchain bitcoin reste néanmoins la traçabilité[1].

Une transaction en bitcoin est l'équivalent d'un paiement sous pseudonyme, le pseudonyme étant la clé publique utilisée pour acquérir ou céder des unités de valeur. Chaque utilisateur n'intervient qu'à partir de sa clé publique. A partir du moment où une clé publique est reliée à l'identité d'une personne physique, la blockchain bitcoin peut permettre de remonter l'intégralité des transactions de cet utilisateur. Un intervenant sur la blockchain - banque, commerçant, administration – qui connaît à la fois l'identité d'une personne et sa clé publique, peut croiser ses propres données clients avec les données transactionnelles issues de la blockchain. Au fur et à mesure que l'utilisation de la blockchain bitcoin se banalise, les outils logiciels d'analyse des transactions se développent.

C'est pourquoi les experts attachés à un anonymat total cherchent à développer d'autres blockchains. Certaines blockchains ont été spécialement conçues pour rendre les transactions intraçables et favoriser le commerce opaque. Les méthodes de préservation de l'anonymat reposent sur différentes technologies cryptographiques complexes.

L'une de ces blockchains repose sur une technique appelée *zero knowledge proof*. Elle consiste à éclater les données d'une transaction en un grand nombre de sous-ensembles, qui seront mélangés entre eux, selon un principe comparable à celui du *clouding*, afin de rendre une transaction intraçable.

Une autre blockchain repose sur la technique dite *one time ring signature*. Elle utilise un système de clés circulaires qui empêche d'identifier, lors de la validation, l'émetteur d'une transaction. De même, elle empêche d'identifier le destinataire du paiement en utilisant non sa clé publique, mais une adresse à usage unique. L'opacité est totale.

En revanche, l'identification redevient possible dès qu'un utilisateur cherche à sortir ses valeurs d'une telle blockchain pour les convertir en monnaie réelle ou vers une autre blockchain plus transparente.

LES CARTES DE PAIEMENT EN MONNAIE RÉELLE ADOSSÉES À DES COMPTES EN BITCOIN (CARTES DITES « BITCOIN TO PLASTIC » OU « BTC2PLASTIC »)

Apparues en 2013, les cartes de paiement adossées à des portefeuilles en bitcoins (BTC), dites cartes « BTC2plastic », se développent rapidement. Le solde disponible sur la carte est équivalent à la contre-valeur en monnaie réelle du montant de bitcoins détenus. Ces cartes permettent de payer en monnaie réelle auprès d'un commerçant physique ou en ligne, ou de retirer des espèces dans les distributeurs automatiques des réseaux VISA et Mastercard. Cette dernière fonction,

1 Cf Laurent LELOUP, *Blockchain, la révolution de la confiance*, Eyrolles, 2017 (p.50 à 55)

dite de *cash out*, est utilisée par les criminels pour retirer en espèces les profits illicitement acquis en bitcoins. Ces profits sont le plus souvent issus de la vente de produits interdits sur le *darkweb* (stupéfiants, armes, faux documents d'identité, coordonnées bancaires volées...).

Ces cartes posent un problème similaire à celui des cartes prépayées rechargeables en espèces. Elles offrent un degré élevé d'anonymat et une portabilité maximum. Le risque LCB/FT ne peut être limité que par un haut niveau de conformité des sociétés émettrices quant à leurs obligations de vigilance, ce qui n'est pas acquis dans le cas des émetteurs identifiés à ce jour. Il existe au moins une vingtaine d'opérateurs de cartes BTC2plastic, implantés à l'étranger (Amérique, Asie, espace russophone). La moitié d'entre eux ont recours au même établissement de monnaie électronique, immatriculé dans une place off-shore méditerranéenne.

Certains opérateurs de cartes BTC2plastic acceptent de coopérer avec les autorités. D'autres sont plus fermés et font de la garantie de l'anonymat un argument commercial central. S'ils affichent dans leurs conditions générales d'utilisation des seuils au-delà desquels existent des mesures d'identification, ils n'appliquent en réalité que des mesures de contrôle dégradées.

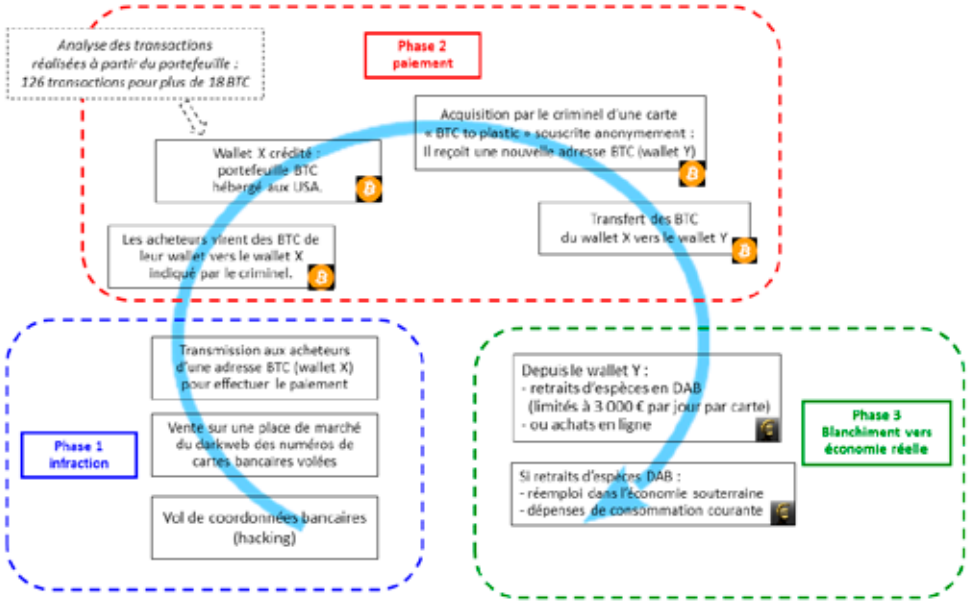
Le cybercriminel pourra choisir une offre qui préserve l'anonymat complet du porteur de la carte. De plus, les éventuels seuils de chargement, de paiement et de retrait sont aisément contournés grâce à l'ouverture d'un nombre illimité de comptes. Les services d'enquête peinent à identifier les porteurs, d'autant que ceux-ci maximisent souvent les précautions avec l'utilisation du réseau TOR et de réseaux privés virtuels (VPN).

Cas n°36

Au sein de la Gendarmerie Nationale, le Service Central du Renseignement Criminel (SCRC) dispose d'une unité de police judiciaire spécialisée, le Centre de lutte Contre les Criminalités Numériques (C3N), avec lequel Tracfin coopère. Cette unité a conduit depuis deux ans plusieurs affaires judiciaires impliquant l'utilisation de cartes BTC2plastic.

Le 17 février 2016, le C3N a procédé à l'interpellation d'un cybercriminel français proposant à la vente sur le *darkweb* des numéros de cartes bancaires volés, contre paiement en bitcoins. Les recettes des ventes étaient transférées sur un portefeuille bitcoin rattaché à une carte BTC2plastic émise à l'étranger. Ces fonds étaient par la suite retirés en espèces à un distributeur automatique de billets ou dépensés pour l'achat de matériels informatiques sur Internet.

- Les fonds ne passent pas par le système bancaire classique.
- Les transactions et les retraits DAB ne sont détectables que par une réquisition auprès de l'émetteur de la carte, du changeur monnaie réelle/monnaie virtuelle, ou de l'Emetteur de Monnaie Electronique gérant le portefeuille de monnaie électronique réelle.
- Les seuils de contrôle prévus par la réglementation sur la monnaie électronique peuvent être contournés par la souscription de plusieurs cartes.
- Identifier les transactions ne signifie pas systématiquement identifier le délinquant. Ce dernier peut avoir recours à des techniques d'anonymisation, tant sur Internet (VPN, TOR) que pour d'éventuelles livraisons de biens physiques achetés en ligne (« drop-shipping »).
- Identifier la carte BTC2plastic utilisée ne signifie pas systématiquement identifier son bénéficiaire effectif. La carte peut avoir été souscrite anonymement dans sa version de base.



LES CARTES DE PAIEMENT ADOSSÉES AUX MATIÈRES PREMIÈRES : CARTES « COMMODITIES TO PLASTIC »

Lancé en 2013, un service conçu et commercialisé par un négociant en métaux précieux permet à son utilisateur d'acheter de l'or, de l'argent ou des diamants afin de constituer une épargne liquide, tangible et hors système bancaire. Les matières précieuses sont conservées en coffre-fort, en Suisse. En contrepartie de ses valeurs, le client se voit remettre une carte prépayée de paiement, dont le montant d'emport est indexé sur les matières premières physiquement détenues[1].

La carte prépayée est techniquement émise par un PSP de droit anglais et adossée au réseau MasterCard. Le PSP exerce son activité en France sous le régime de la libre prestation de services (LPS). Le contrat liant le négociant en métaux précieux et le PSP est régulé par le superviseur britannique (Financial Conduct Authority).

Selon la documentation disponible, cette carte de paiement ne semble pas comporter de plafond d'emport, ce qui serait contraire au CMF qui fixe à 10 000 € le montant maximum de stockage de monnaie électronique sur un support physique. Les paiements sont par défaut plafonnés à 500 € par jour, mais ce plafond peut être relevé sur simple demande du client.

En tant que négociant en métaux précieux, la société qui commercialise la carte est tenue de respecter ses obligations LCB/FT sur le territoire français, telles que la prise d'identité de ses utilisateurs et la déclaration d'opérations suspectes[2]. De plus, elle tient un registre de police de toutes les transactions d'achat et de vente. Le dispositif reste cependant fragile. Des fraudes documentaires ou à la carte bancaire ont été constatées.

Tracfin a pu établir que ce type de carte avait été utilisé par un individu soupçonné de départ vers la zone de conflit au Proche-Orient.

1 Dans le cas des diamants, l'absence de cours officiel et la difficulté de coter les pierres posent le même problème d'évaluation que celui mentionné en p.18 du présent rapport.

2 Cf 11° de l'article L.561-2 du code monétaire et financier

LES PLATES-FORMES DE CHANGE ENTRE MONNAIES VIRTUELLES ET MATIÈRES PREMIÈRES (COMMODITIES TO CRYPTOMONEY)

Une plate-forme de e-commerce immatriculée dans un pays de l'UE permet d'acheter et de revendre des métaux précieux tels que l'or, l'argent, le platine ou le palladium. La plate-forme accepte les paiements en monnaies virtuelles : bitcoins, ethers, ripple.

Une CRF étrangère a informé Tracfin qu'un individu résidant en France avait blanchi des revenus en bitcoins issus d'activités de *carding* (revente de coordonnées bancaires volées) en les convertissant en métaux précieux via cette plateforme.

Les matières premières comme l'or et les diamants sont des vecteurs avérés de blanchiment. Toute technologie qui facilite leur conversion en moyens de paiement, qu'il s'agisse de monnaie électronique ou de monnaie virtuelle, est un facteur d'accroissement du risque.

LE TRANSFERT INTERNATIONAL EN PEER-TO-PEER : LA CRÉATION D'« ESPÈCES NUMÉRIQUES »

Certaines plateformes ont également profité de la technologie blockchain pour proposer des services de transfert international de fonds à moindre coût.

Cas n° 37

Une plateforme américaine propose ainsi aux particuliers des transferts de fonds internationaux en monnaie réelle, en s'identifiant uniquement par un numéro de téléphone. La plate-forme convertit les fonds du client en bitcoins, puis utilise la blockchain pour effectuer une transaction de pair à pair, les fonds étant in fine reconvertis dans la monnaie réelle du destinataire. Le passage par la monnaie virtuelle est insensible pour les utilisateurs, qui ne sont pas tenus de gérer eux-mêmes un portefeuille de monnaie virtuelle.

Concrètement, un utilisateur souhaitant effectuer un transfert de fonds à l'étranger a plusieurs possibilités :

- Les utilisateurs, expéditeurs comme bénéficiaires, doivent préalablement ouvrir un compte de monnaie électronique auprès de l'opérateur.
- Lors de l'ouverture d'un compte, la plateforme crée parallèlement un portefeuille bitcoin en générant les

clés cryptographiques nécessaires. La clé publique correspond à l'adresse du portefeuille bitcoin utilisé pour les transactions d'un client, et sera reliée au compte de monnaie électronique et au numéro de téléphone de celui-ci. Le numéro de téléphone sera le seul moyen d'identification du client par les autres membres de la communauté d'utilisateurs.

- Le compte se charge de deux manières :

  Schéma A.
  – soit depuis un compte bancaire en effectuant un virement bancaire vers le compte de monnaie électronique ouvert sur la plateforme ;

  Schéma B.
  – soit directement en espèces, auprès d'autres utilisateurs du service, localisables de la même manière qu'un chauffeur sur une plateforme collaborative de transport. Les utilisateurs volontaires peuvent en effet assurer la fonction d'agents de change : en échange d'espèces, ils créditent d'un montant équivalent en bitcoins le portefeuille bitcoin d'un autre utilisateur.

- L'utilisateur communique ensuite le numéro de téléphone du bénéficiaire, qui reçoit les fonds sur son compte préalablement ouvert.
- Le bénéficiaire peut transférer la somme sur son compte bancaire ou bien la récupérer en espèces selon le même principe d'échange entre membres de la communauté de volontaires.

Ainsi, lorsqu'un transfert a pour origine une alimentation en espèces et pour destination un retrait d'espèces, l'anonymat, garanti par la conversion en bitcoins, est largement préservé. Seul le numéro de téléphone et la clef cryptographique publique sont connus de la plateforme. Les espèces de part et d'autre de la transaction sont « numérisées » par leur conversion en monnaie virtuelle.

Cette plateforme n'est pas encore disponible en Europe à ce jour mais pourrait rapidement le devenir.

Schéma A.

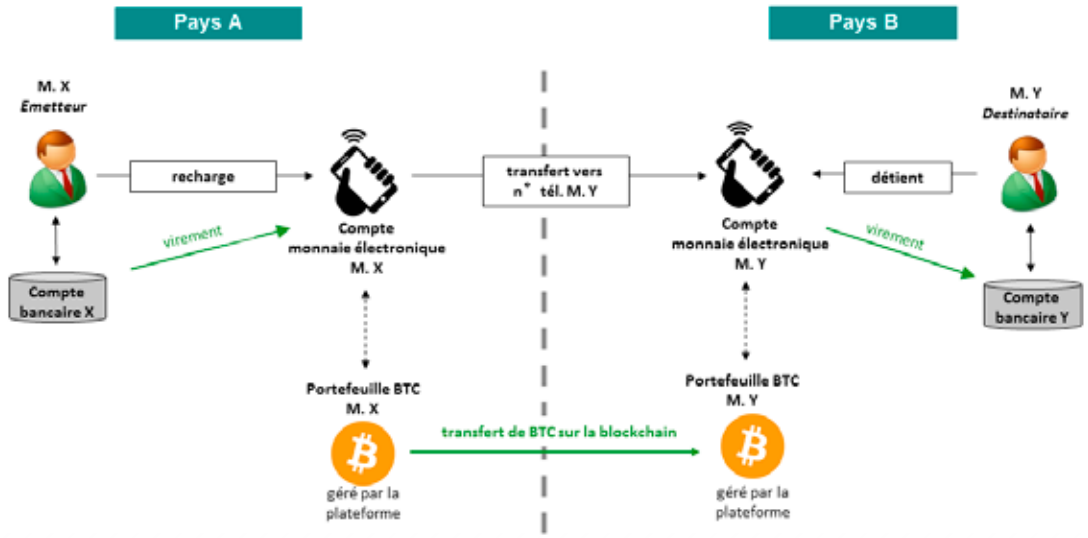
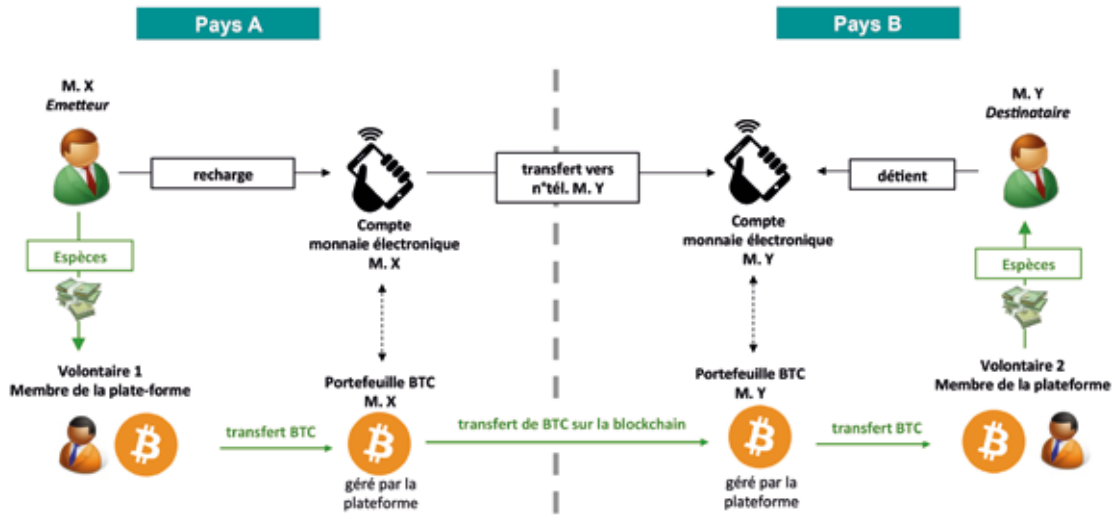


Schéma B.



LA FRAUDE À L'IDENTITÉ ET LA FRAUDE DOCUMENTAIRE : UNE FAILLE D'AMPLEUR

Si les innovations technologiques tendent à faciliter l'anonymat, le premier facteur d'anonymat dans les services de paiement reste la fraude documentaire et la fraude à l'identité. L'ampleur de ce phénomène constitue aujourd'hui une faille sérieuse dans les procédures de connaissance client (KYC), en particulier pour les services de paiement en ligne. Il est aisé de se procurer sur internet - ou via une officine - de faux documents d'identité dont la qualité et la véracité ne pourront que difficilement être authentifiées par un opérateur ; d'autant que les dispositifs de vérification d'identité des clients mis en œuvre par certains prestataires de services de paiement sont peu efficaces.

Le recours aux faux documents d'identité se conjugue à l'utilisation des nouvelles technologies favorisant l'anonymat :

- Dans le champ des monnaies virtuelles, les déclarations de soupçon reçues par Tracfin font état d'un nombre important d'utilisation de documents falsifiés ou volés pour accéder aux plateformes de change entre monnaie réelle et monnaie virtuelle. Ceci témoigne d'intentions frauduleuses. L'utilisation de fausses pièces d'identité à l'entrée en relation, et parfois l'utilisation de VPN[1] pour masquer l'adresse IP de l'utilisateur, permettent aux utilisateurs de s'assurer d'un anonymat total dans leurs opérations.
- Dans le champ du financement participatif, Tracfin constate également des tentatives d'utiliser de faux documents d'identité sur les plateformes de *crowdfunding*. Les prestataires de services de paiement agréés en France, qui gèrent les comptes des plateformes, sont informés des risques : lorsqu'ils détectent des fraudes à l'identité, ils refusent d'ouvrir un compte de paiement.

Les plateformes de *crowdfunding* sont également vulnérables à l'utilisation de cartes bancaires volées, fréquemment réutilisées sur ces sites. Des comptes de paiement associés à des sites de collecte sont utilisés comme comptes de passage afin de faire transiter des fonds issus de cartes bancaires volées. Deux typologies se présentent : soit l'individu crée un compte de paiement sans contribuer à un projet et l'utilise simplement comme compte de passage, soit un projet est créé spécialement pour écouler des fonds tirés d'une carte volée.

Un cas a démontré que certains individus utilisent différents sites de cagnotte simultanément afin de fractionner les montants et de ne pas attirer l'attention de l'établissement de paiement. Les montants demeurent faibles et dépassent rarement 1 000 €.

1 VPN : réseau virtuel privé permettant de créer un lien direct entre des ordinateurs distants sans révéler leur localisation.

LES NOUVELLES TECHNOLOGIES ÉLARGISSENT EN PERMANENCE LE CHAMP DES POSSIBLES EN MATIÈRE D'ESCROQUERIES

L'USAGE PERVERTI DES *BLOCKCHAINS* POUR LA FRAUDE ET L'ESCROQUERIE

L'analyse des déclarations de soupçon portant sur l'usage de monnaies virtuelles révèle des cas récurrents d'escroqueries : soit des escroqueries pyramidales de type Ponzi, soit des opérations de manipulation de cours sur l'unité de compte d'une blockchain.

En ce sens, les blockchains ne créent pas véritablement de nouvelles méthodes d'escroquerie mais offrent un nouveau champ d'application pour des méthodes éprouvées.

L'escroquerie simple : la *blockchain* fictive

Courant 2016, Tracfin a reçu plusieurs déclarations de soupçon concernant une prétendue blockchain, relevant de la simple escroquerie de type Ponzi.

Les créateurs de cette blockchain proposaient aux investisseurs d'acheter sur internet des unités de valeur en monnaie virtuelle alors que la dite blockchain n'avait jamais été développée et n'avait aucune existence réelle. Il s'agissait d'un simple site internet. La prétendue monnaie virtuelle était commercialisée par une société domiciliée dans le Golfe Persique et détenant des comptes bancaires dans un pays de l'UE.

Les escrocs sont parvenus à collecter plusieurs dizaines de millions de dollars dans le monde entier, une partie des fonds ayant été consacrée à assurer la promotion du site. Ils avaient enrôlé une personnalité politiquement exposée d'un pays membre de l'Union Européenne pour assurer leur promotion. Une plainte pour escroquerie a été déposée contre cet élu.

Si ce cas a été médiatisé, Tracfin a eu connaissance de plusieurs autres sites internet du même type, proposant des blockchains fictives.

L'escroquerie subtile : la manipulation de cours par prise de contrôle rampante des processus de validation de transactions au sein d'une blockchain

Les concepteurs d'une blockchain ont mis en œuvre un mécanisme d'escroquerie subtile, reposant sur un changement de méthode pour valider les transactions, ce qui leur a permis de manipuler les cours.

LA VALIDATION DES TRANSACTIONS SUR UNE BLOCKCHAIN : LES MÉCANISMES DE CONSENSUS

Une blockchain, en tant que registre décentralisé, repose sur la validation des transactions par l'ensemble de ses membres. La validation d'une série de transactions (un bloc) est appelée minage. Le mineur qui valide un bloc reçoit une récompense sous la forme d'un montant de l'unité de valeur en vigueur sur la blockchain concernée.

Il existe deux grandes méthodes de validation des transactions :

– La méthode la plus sûre est appelée *Proof of Work* (preuve de travail).

En vigueur sur la blockchain bitcoin, elle prend la forme d'une énigme mathématique à résoudre par tous les participants de la chaîne qui le souhaitent, chacun ayant au départ les mêmes chances de parvenir à résoudre l'énigme en premier.

Au lancement d'une blockchain, quand il y a peu de transactions, le *Proof of Work* est relativement simple. Plus le réseau s'étend, plus il devient complexe.

– Une autre méthode est appelée *Proof of Stake* (preuve d'enjeu).

Cette méthode consomme moins de puissance de calcul. Elle consiste à créer un mécanisme qui punit les nœuds du réseau qui ne suivent pas le protocole de consensus. Pour avoir le droit de valider les blocs, les participants misent un montant d'unité de valeur sur le résultat attendu du consensus. Si ce résultat n'a pas lieu, les nœuds malveillants qui avaient parié contre le consensus majoritaire perdent leur mise. Ceux qui tentent de

tricher en validant un bloc qui ne devrait pas être validé sont pénalisés financièrement.

Cette seconde méthode est cependant critiquée pour deux raisons. D'une part elle est considérée comme moins sûre et plus vulnérable aux attaques ; d'autre part, elle a un fonctionnement « censitaire » : la probabilité d'être choisi pour miner un bloc dépend de la quantité d'unités de valeur déjà possédée par le mineur.

La méthode *Proof of stake* apparaît donc comme un système propriétaire, privatisé par les possesseurs de coins. La validation des transactions repose sur ceux qui possèdent déjà les coins, de la même façon que les droits de vote au conseil d'administration d'une société anonyme appartiennent à ceux qui détiennent les actions.

Source : Stéphane Loignon, *Big bang blockchain, la seconde révolution d'internet*, Tallandier, 2017.

Les créateurs de la blockchain concernée ont initialement choisi la méthode du *Proof of Work*. Ils ont miné eux-mêmes et ont capté 80% des coins générés sur leur blockchain. Puis, ils ont basculé en *Proof of Stake*. Comme ils détenaient la majorité des coins générés sur leur blockchain, ils étaient en mesure de contrôler la validation des transactions.

Les concepteurs de cette blockchain ont alors pu procéder à des opérations de *pump and dump*, c'est-à-dire des manipulations de cours consistant à faire gonfler artificiellement le cours de l'unité de valeur, à revendre ces coins au cours le plus haut, puis à laisser la valeur s'effondrer. En effet, quelques acteurs complices et pesant d'un certain poids sur un marché donné, peuvent s'entendre pour enchaîner des transactions destinées à attirer des petits investisseurs (suiveurs) en créant de l'activité et de la hausse sur les unités de valeur. La capitalisation - ou valeur totale - des coins de cette blockchain est ainsi montée jusqu'à 32 M$. Les détenteurs les ont alors cédés contre des bitcoins. Les cours sont vite retombés, lésant les derniers acquéreurs.

On estime que les fondateurs d'un tel site sont parvenus à céder leurs coins à temps, obtenant une contrevaleur d'environ 20 M$ en bitcoins. Ils ont pu la convertir anonymement en monnaie réelle en utilisant des cartes BTC to plastic. Ces revenus n'ont laissé aucune trace et n'ont été soumis à aucune fiscalité.

Lorsque la blockchain qui sert à ce type de manœuvres devient négativement connue, les concepteurs peuvent procéder à plusieurs changements de noms ou la convertir vers d'autres applications, comme l'utilisation des coins sur des plateformes de e-commerce.

Par souci de discrétion et de faisabilité technique, les escrocs ont tendance à privilégier les blockchains ayant de faibles capitalisations, ainsi que les plates-formes de marché de second rang. La blockchain bitcoin, par son importance, peut sembler trop visible ou exiger trop de puissance de calcul. Cependant, l'emballement du cours du bitcoin sur le premier semestre 2017 empêche d'exclure totalement la possibilité de manipulation de cours sur cette monnaie. L'existence d'acteurs influents (coopératives de mineurs, développeurs reconnus, acteurs industriels) peut nuire, au moins en théorie, à la décentralisation du système.

LES RISQUES D'ESCROQUERIE SE DÉVELOPPENT DANS LE *CROWDFUNDING* AVEC LA BANALISATION DES PLATES-FORMES DÉDIÉES.

De la même façon que pour les monnaies virtuelles, les déclarations de soupçon reçues par Tracfin en 2016 établissent plusieurs cas d'escroquerie de type Ponzi qui pèsent sur la réputation des plateformes de *crowdfunding*. Le non-remboursement des prêts proposés en ligne nuit à la crédibilité de leur offre. Ceci constitue aujourd'hui le levier qui incite les Intermédiaires en Financement Participatif (IFP) à mettre en œuvre le dispositif LCB/FT et à effectuer des déclarations de soupçon.

Tracfin a transmis en justice le cas d'une plateforme établie au Royaume-Uni, gérée par un Français, qui est parvenue à lever plus de 700 000 € auprès de particuliers. Pour l'essentiel, les fonds ont été utilisés par le gérant et non investis dans les projets affichés.

Les IFP ont signalé d'autres types d'escroqueries : des cas de PME demandant des prêts sur la base de faux documents (factures, identité, ...) mais aussi des cas de non-remboursement des prêts décaissés. Une société a notamment réalisé une demande de prêt auprès d'une plateforme et n'a honoré que trois échéances de remboursement sur vingt-quatre. La société a été placée en liquidation judiciaire peu après l'obtention du prêt et les gérants ont quitté la France pour la Turquie. Le préjudice à l'encontre de la plateforme s'élève à environ 50 000 €.

L'ACTIVITÉ DE TRACFIN EN MATIÈRE DE MONNAIE VIRTUELLE ET DE *CROWDFUNDING*

En 2016, Tracfin a reçu 178 déclarations de soupçon directement liées à des transactions en monnaie virtuelle pour un total de près de 5 M€.

Dans plus de la moitié des cas, l'utilisation de monnaies virtuelles (achat ou vente) est l'élément à l'origine de la déclaration de soupçon. La majorité des déclarations ont pour motif un doute sur l'origine ou la destination de fonds sans caractérisation précise du soupçon.

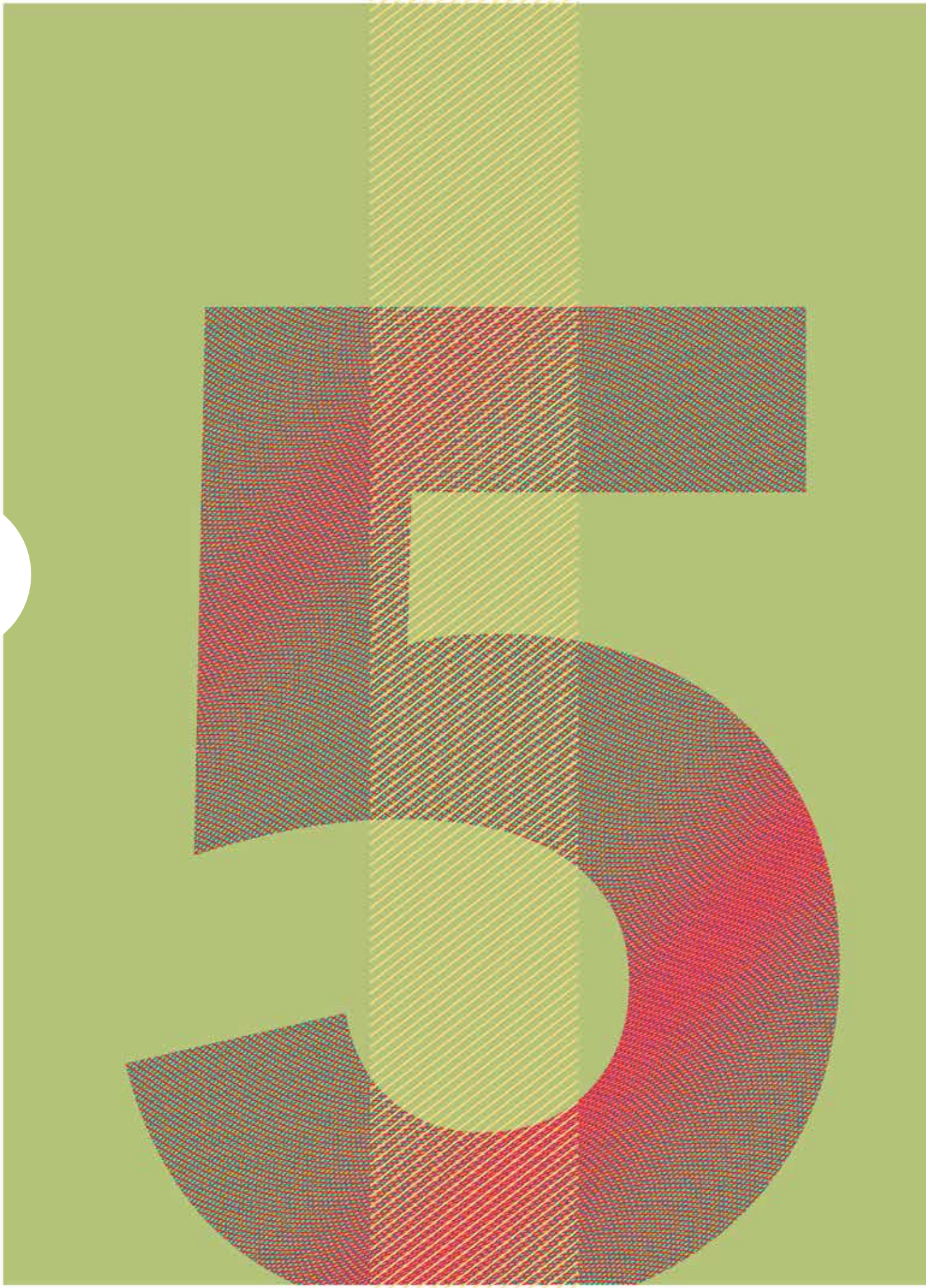
Les phénomènes les plus régulièrement recensés par les déclarants sont des cas d'intermédiation ou d'exercice illégal d'une profession réglementée[1]. Ces dossiers font état d'individus collectant des fonds en provenance de nombreux particuliers dans le but de procéder à des opérations d'achat/revente de monnaies virtuelles sur des plateformes d'échange européennes pour le compte de tiers.

En matière de *crowdfunding*, en 2016, Tracfin a reçu 149 déclarations de soupçon concernant le financement participatif et les cagnottes en lignes. Ce chiffre est en forte hausse. L'augmentation du flux en 2016 est due au recours croissant des particuliers à ces plateformes et à la sensibilisation des assujettis aux risques LCB/FT. Si les montants investis dans les cagnottes dépassent rarement les 1 000 €, les investissements réalisés par des particuliers sur des plateformes de financement participatif peuvent atteindre plusieurs dizaines de milliers d'euros.

Les typologies détectées au sein des déclarations de soupçon reçues en 2016 présentent une diversité plus importante qu'en 2015, reflétant la multiplication des plateformes et la croissance de leur utilisation. L'utilisation la plus simple d'une plateforme de *crowdfunding* à des fins de blanchiment consiste, pour une personne physique, à investir sur la plateforme afin de contribuer à des projets dont il est lui-même porteur. Un établissement de paiement a ainsi détecté un particulier qui avait ainsi fait circuler plus de 250 k€. Les cas de soupçon de financement du terrorisme, présents depuis 2014, sont en augmentation.

Les établissements de paiement et les établissements de monnaie électronique partenaires des plateformes de *crowdfunding* semblent particulièrement mobilisés et conscients des risques qui peuvent peser sur leur réputation dans le cas d'utilisations frauduleuses de ces plateformes.

1 En l'occurrence la profession d'Intermédiaire en Opération de Banque et de Service de Paiement (IOBSP).



MESURES D'ATTÉNUATION DES RISQUES : LES AUTORITÉS FRANÇAISES ADAPTENT LA RÉGLEMENTATION, DONT L'EFFICACITÉ RESTE CONDITIONNÉE À LA QUALITÉ DE LA CONCERTATION INTERNATIONALE

L'ANNÉE 2016 A ÉTÉ MARQUÉE PAR UNE ACTIVITÉ LÉGISLATIVE ET RÉGLEMENTAIRE SOUTENUE, EN PARTICULIER POUR MIEUX ENCADRER LA MONNAIE ÉLECTRONIQUE ET LES CARTES PRÉPAYÉES

Le législateur français a mené une action résolue en 2016 pour mieux encadrer l'émission de monnaie électronique et l'utilisation des cartes prépayées[1]. Compte-tenu du contexte terroriste, le législateur français a anticipé sur la législation LCB/FT européenne en publiant en 2016 plusieurs textes destinés à mieux encadrer l'usage de la monnaie électronique.

– Depuis le 1er janvier 2017, toute opération de paiement en monnaie électronique en France, par carte ou depuis un serveur, est plafonnée à 3000 €[2].

– La transposition de la 4e directive a permis de réduire l'anonymat de la monnaie électronique :

- Tout support physique de paiement alimenté depuis des moyens de paiement traçables (compte bancaire nominatif ouvert dans un pays de l'Espace Economique Européen) nécessite une prise d'identité dès que le rechargement dépasse 250 € par mois. Les remboursements en espèces sans vérification d'identité ne sont possibles que jusqu'à 100 €.
- Tout support physique de paiement alimenté depuis des moyens de paiement non traçables (espèces ou monnaie électronique anonyme) doit faire l'objet d'une prise d'identité au premier euro, à chaque rechargement. La seule exception concerne les cartes « enseignes », utilisables uniquement en France pour l'achat de biens et services limités, qui peuvent être chargées en espèces sans vérification d'identité jusqu'à 250 € par mois[3].
- Pour les services de paiement en ligne, les opérateurs sont dispensés de prise d'identité uniquement pour les paiements en ligne d'un compte bancaire de l'EEE vers un autre compte bancaire de l'EEE, pour des opérations de moins de 250 €, et dans la limite de 2 500 € par an[4].

– L'utilisation des cartes prépayées a été encadrée par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement[5]. Un décret a défini des plafonds d'utilisation[6] :

- une carte ne peut être chargée de plus de 10 000 € ;
- les rechargements en espèces sont limités à 1 000 € par mois ;
- les retraits ou les remboursements de solde en espèces sont également limités à 1 000 € par mois.

De plus, la loi oblige les établissements à conserver cinq ans les informations clients relatives à l'activation, au chargement et à l'utilisation de la monnaie électronique au moyen d'un support physique[7].

Les évolutions apportées au cadre juridique de la monnaie électronique limitent progressivement les risques inhérents aux cartes prépayées. L'année 2016 a également permis de consolider le dispositif LCB/FT grâce à la transposition en droit français de la 4e directive européenne LCB/FT, par l'ordonnance n°2016-1635 du 1er décembre 2016[8].

Bien que ce renforcement de la législation soit encore trop récent pour en mesurer pleinement les effets, il ne s'agit vraisemblablement que d'une première étape. Le dispositif restera vulnérable sans une harmonisation renforcée des exigences réglementaires et des pratiques professionnelles, au plan européen comme international.

1 Pour une présentation détaillée de ces mesures : Cf Annexe n°1

2 Décret n°2016-1985 du 30 décembre 2016 modifiant l'art. D.112-3 du CMF

3 Art. R.561-16 du CMF

4 Art. R.561-16-1 du CMF. Les articles R.561-16 et R.561-16-1 du CMF pourraient être prochainement remaniés et le seuil de 250 € abaissé.

5 Loi n°2016-731 du 3 juin 2016, dite « loi Urvoas », notamment sa disposition modifiant l'art. L.315-9 du CMF.

6 Décret n°2016-1742 du 15 décembre 2016, transcrit dans l'art. D.315-2 du CMF.

7 Art. L.561-12 du CMF. A fin juin 2017, cette disposition devait encore être précisée par décret.

8 Cf Annexe n°2

L'INDISPENSABLE RESPONSABILISATION DES NOUVEAUX ACTEURS DU PAIEMENT

La mise en place des filières de conformité LCB/FT au sein des établissements bancaires s'est accélérée au tournant des années 1990-2000 et a nécessité entre cinq et dix ans pour atteindre un mode de fonctionnement relativement efficace. Ce chantier est aujourd'hui rouvert auprès des nouveaux acteurs des services de paiement. Ceux-ci, consacrés par la DSP2, n'ont pas la même culture du risque de blanchiment que les établissements bancaires et font même, pour certains, de la levée des contraintes réglementaires un ressort de leur développement.

LES NOUVEAUX PRESTATAIRES DE SERVICES DE PAIEMENT : UNE CULTURE DE CONFORMITÉ À CONFORTER

La responsabilisation des nouveaux acteurs du paiement sur les problématiques de blanchiment et de financement du terrorisme est nécessaire à l'efficacité et à la cohérence du dispositif LCB/FT. Leur encadrement réglementaire doit être poursuivi.

Comme les autres professionnels assujettis, les Etablissements de Paiement (EP) et les Etablissements de Monnaie Electronique (EME) sont tenus de respecter leurs obligations LCB/FT. L'ACPR a déjà sanctionné certains établissements pour, entre autres, non-respect de leurs obligations de vigilance et d'identification client[1].

Ces obligations importent particulièrement dans le cas des PSP qui utilisent des réseaux d'agents (pour les services de paiement) ou de distributeurs (pour la monnaie électronique). Le PSP doit veiller à la conformité des membres de ses réseaux de distribution. Ces derniers ne sont pas des professionnels financiers et sont trop peu sensibilisés au risque LCB/FT.

Par exemple, la vente de tickets ou de coupons prépayés en espèces et destinés à recharger des *wallets* électroniques met en lumière les limites des dispositions prises pour lutter contre l'anonymat dans l'usage de la monnaie électronique. Certains distributeurs de monnaie électronique peuvent faire une interprétation extensive de la notion de réseau d'utilisation limité pouvant s'appliquer à une carte de paiement, afin de ne pas avoir à identifier le client.

La concurrence entre PSP peut aussi les inciter, auprès de leurs agents et distributeurs, à privilégier le développement commercial au détriment des obligations LCB/FT. En ce sens, les agents et distributeurs multimarques sont les plus sensibles.

LES PLATES-FORMES DE MARCHÉ EN MONNAIES VIRTUELLES : UNE CULTURE DE CONFORMITÉ À FAIRE NAÎTRE

Les places de marché assurent la conversion entre monnaie réelle (fiat) et monnaie virtuelle (crypto). Elles ont une responsabilité importante en matière d'identification client. Elles peuvent décider de faciliter ou non l'anonymat des transactions en monnaies virtuelles, en fonction de l'exigence des procédures d'identification client qu'elles mettent en place.

Les plates-formes de marché et les fournisseurs de portefeuille (*wallet providers*) sont d'importants pourvoyeurs de clés publiques et privées à destination des utilisateurs. Ces acteurs ont la même responsabilité en matière d'identification client qu'un PSP lorsqu'il propose à un client d'ouvrir un *wallet* de monnaie électronique.

Les plates-formes de marché actuellement établies en France collectent un degré d'information client variable selon le montant des transactions. Pour des montants faibles, les plates-formes identifient le client en collectant un nom, une adresse postale et une référence de compte bancaire (RIB ou IBAN). Mais la vérification d'identité n'est pas systématique. Elle le devient lorsque les montants sont plus importants, selon des seuils variables en fonction des plates-formes, en exigeant la production d'une pièce d'identité.

Le législateur français a souhaité impliquer ces acteurs dans la lutte contre le blanchiment et le financement du terrorisme. Depuis l'ordonnance de transposition n°2016-1635 du 1er décembre 2016, les plates-formes de marché et les *wallet providers* immatriculés en France

1 Cf procédure n°2014-10 du 16 octobre 2015, et procédure n°2016-05 du 3 mars 2017, disponibles sur le site internet de l'ACPR, rubrique « Commission des sanctions ».

sont assujettis au dispositif LCB/FT (cf 7°bis de l'art. L.561-2 du CMF[1]). Ils doivent donc mettre en place des procédures d'identification et de vérification d'identité, ainsi que des mesures de vigilance adéquates.

Sur ce point, le législateur français a anticipé sur le législateur européen. Cette obligation n'est pas incluse dans la directive (UE) 2015-849 (4ème directive antiblanchiment). Des discussions sont actuellement en cours à Bruxelles pour la préparation d'une nouvelle version de la directive antiblanchiment (appelée 4ème bis ou 5ème directive), qui devrait imposer l'assujettissement des opérateurs de monnaies virtuelles dans l'ensemble des pays de l'UE.

Cependant, l'assujettissement de ces professionnels en France n'est qu'un premier pas. Leur encadrement réglementaire reste incomplet dans la mesure où ils ne sont soumis à aucune procédure d'agrément. Aucune autorité de contrôle dédiée n'a encore été désignée sur ce secteur. Enfin, le dispositif restera peu efficace tant que des règlementations similaires ne se développeront pas à l'échelle internationale.

1 Le 7°bis de l'article L.561-2 du CMF définit ainsi les opérateurs de monnaie virtuelle : « Toute personne qui, à titre de profession habituelle, soit se porte elle-même contrepartie, soit agit en tant qu'intermédiaire, en vue de l'acquisition ou de la vente de tout instrument contenant sous forme numérique des unités de valeur non monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur. »

LA SUPERVISION DES NOUVEAUX ACTEURS EST LIMITÉE PAR LE PASSEPORT EUROPÉEN ET COMPLIQUÉE PAR L'ÉVOLUTION DU SECTEUR

L'émergence des nouveaux acteurs du paiement, l'utilisation de la monnaie électronique et de la monnaie virtuelle et l'absence de logique géographique mettent au défi le cadre réglementaire. Un dispositif efficace de contrôle doit couvrir la totalité de la chaîne des acteurs. Toute rupture géographique (un opérateur localisé dans un pays non coopératif) ou fonctionnelle (un des opérateurs de la chaîne non assujetti aux obligations en matière de LCB/FT) induit une fragilité structurelle du dispositif de surveillance.

LE PASSEPORT EUROPÉEN ET LE RÉGIME DE LA LIBRE PRESTATION DE SERVICES LIMITENT LA SUPERVISION ET LE CONTRÔLE DES NOUVEAUX ACTEURS DU PAIEMENT

Les autorités françaises sont conscientes qu'avec la révolution digitale, le dispositif LCB/FT restera d'une efficacité limitée s'il ne se développe pas à l'échelle internationale.

Même au seul niveau européen, l'efficacité du dispositif est limitée par le passeport européen, qui permet aux opérateurs de distribuer leurs produits dans l'ensemble de l'EEE, tout en étant agréé dans un seul pays. Or le cadre européen commun n'est pas appliqué de manière homogène par tous les pays membres. La mise en œuvre des obligations LCB/FT incombant aux opérateurs n'est pas encadrée avec la même efficacité par les autorités de contrôle des différents pays de l'UE.

Le passeport européen permet à une entreprise agréée dans un État membre de l'Espace Économique Européen (pays d'origine) d'offrir ses services sur le territoire d'un autre État membre (pays d'accueil) :

– soit en Libre Etablissement (LE) à partir d'un établissement permanent dans le pays d'accueil, par exemple une succursale ou une agence, et/ou en ayant recours à des agents ou des distributeurs ;
– soit en Libre Prestation de Services (LPS) sans être établi dans le pays d'accueil, en proposant ses services en ligne.

En Libre Etablissement, les organismes financiers sont soumis aux réglementations nationales relatives à la LCB/FT et à la protection de la clientèle. En France, ceux qui ont recours à des agents ou à des distributeurs de monnaie électronique, doivent désigner un correspondant permanent dont la fonction est d'être l'interlocuteur de Tracfin et de l'ACPR[1].

Les autorités de supervision françaises sont compétentes pour contrôler le respect de ces dispositions. L'ACPR contrôle et sanctionne des succursales exerçant en LE et, depuis 2016, procède au contrôle de réseaux d'agents et de distributeurs.

En revanche, en Libre Prestation de Services, le superviseur national n'est pas compétent pour contrôler les établissements étrangers exerçant sur son territoire. Ceux-ci doivent se conformer à la règlementation de leur pays d'origine. En cas de doute, les autorités du pays d'accueil peuvent alerter les autorités du pays d'origine, lesquelles ne sont pas toujours coopératives.

En ce sens, la LPS représente un risque majeur. A fin 2016, la France comptait 594 établissements de paiement ou de monnaie électronique opérant sur son territoire, dont 54 agréés par l'ACPR, 48 exerçant sous le régime du LE, et 492 exerçant sous le régime de la LPS. Une harmonisation du niveau d'exigence des différents superviseurs de l'EEE devient indispensable.

1 art. L.561-3 VI du CMF

	Agrément ACPR	LE	LPS	Total
EP	47	34	381	**462**
EME	7	14	111	**132**
Total	54	48	492	594

Source : chiffres ACPR au 01/01/2017

Au-delà de l'Espace Economique Européen, le dispositif LCB/FT restera vulnérable tant que l'exigence règlementaire ne se développera pas à l'échelle internationale.

LA RÈGLEMENTATION LCB/FT DOIT VEILLER À ASSOCIER, PARMI TOUS LES ACTEURS PROPOSANT DES SERVICES FINANCIERS, CEUX QUI POSSÈDENT LA MEILLEURE CONNAISSANCE CLIENT

Le Comité de Bâle a publié le 31 août 2017 une étude sur l'impact de l'émergence des FinTech sur le marché bancaire[1]. Cette étude propose cinq scénarios sur le devenir des banques, du plus optimiste au plus pessimiste. Un scénario possible conduit à ce que les banques traditionnelles soient progressivement cantonnées à un rôle de prestataire de services informatiques et administratifs, au profit des grands acteurs de l'internet qui s'accapareraient la relation au client final.

La réglementation LCB/FT, si elle est mal calibrée, pourrait à terme tourner à vide et entraîner des distorsions de concurrence au détriment des établissements financiers agréés. Les nouveaux acteurs de l'internet et les opérateurs de téléphonie mobile continueraient de se développer en-dehors du périmètre de la régulation bancaire et concentreraient les données de connaissance client. A l'inverse les banques et les prestataires de services de paiement agréés supporteraient les obligations de conformité et de vigilance LCB/FT, sans pour autant disposer de suffisamment d'informations pour analyser finement les flux.

1 Basel Committee on Banking Supervision : *Sound Practices : Implications of fintech developments for banks and bank supervisors* – Août 2017

ANNEXES

ANNEXE N°1
LE RENFORCEMENT DE L'ENCADREMENT RÉGLEMENTAIRE DE LA MONNAIE ÉLECTRONIQUE MENÉ EN 2016

PLAFOND DE PAIEMENT À 3 000 € POUR TOUTE OPÉRATION EN MONNAIE ÉLECTRONIQUE

Toute opération de paiement en monnaie électronique est plafonnée à 3000 € depuis le 1er janvier 2017.

Six mois après les attentats de janvier 2015, un décret simple avait abaissé le plafond de paiement en espèces ou en monnaie électronique à 1 000 € pour les résidents[1]. Ce décret incluait les paiements électroniques, car à l'époque, les cartes prépayées anonymes n'étaient que très peu encadrées.

Depuis, l'année 2016 a permis de resserrer la réglementation des cartes prépayées (cf infra). Aussi, le 30 décembre 2016, le plafond de paiement en monnaie électronique a-t-il été relevé à 3 000 €[2]. Ce dernier décret est applicable depuis le 1er janvier 2017.

FIN DE L'ANONYMAT

• La règle : la fin de l'anonymat

La règle est que la monnaie électronique émise et distribuée en France ne puisse plus être anonyme, sauf exception précisément définie.

Tout EME voulant distribuer ses produits en France doit se conformer aux articles L.561-5 et L.561-6 du CMF, qui imposent :

– l'identification du client et du bénéficiaire effectif ;
– la vérification de leur identité ;
– la vigilance constante sur la cohérence des opérations de chaque client pendant toute la durée de la relation d'affaires.

Ainsi, toute carte alimentée depuis des moyens non traçables (espèces ou compte de monnaie électronique anonyme) doit faire l'objet d'une prise d'identité au premier euro à chaque rechargement.

Une carte de paiement alimentée depuis des moyens de paiement traçables (carte bancaire ou virement bancaire à partir de comptes bancaires nominatifs ouverts dans un pays de l'EEE) nécessite une prise d'identité pour tous rechargements de plus de 250 € par mois, et dès qu'un retrait ou un remboursement en espèces dépasse 100 €.

• Des exceptions très limitées

L'exception, fixée par l'art. R.561-16 5° du CMF, dispose qu'un support physique de monnaie électronique peut déroger aux articles L.561-5 et L.561-6 du CMF, c'est-à-dire ne pas imposer de vérification d'identité, s'il respecte plusieurs conditions restrictives cumulées :

– il ne sert qu'à régler des biens et des services (pas de transmission de fonds ni d'opérations de change) ;
– il est utilisable uniquement sur le territoire national ;
– il ne peut pas être chargé en espèces ni en ME anonyme (sauf si son usage est réservé à un réseau limité de biens et de services ou d'enseignes) ;
– la limite de stockage (plafond d'emport) est de 250 € ;
– la limite de paiement est également plafonnée à 250 € par mois ;
– la limite de retraits ou de remboursements en espèces est fixée à 100 € par opération.

Ainsi ne peuvent être rechargées en espèces sans vérification d'identité que les cartes émises par certaines enseignes, utilisables uniquement en France dans un réseau de magasins défini, pour l'achat de biens et services limités, et ce pour un montant maximum de 250 € par mois.

Les travaux préparatoires à la modification de la 4e directive prévoient des conditions plus restrictives à la dispense accordée aux émetteurs de monnaie électronique concernant les obligations de vigilance, en abaissant ces divers seuils.

1 Cf décret n°2015-741 du 24 juin 2015 pour l'application de l'art. L.112-6 du CMF

2 Cf décret n°2016-1985 du 30 décembre 2016 pour modifier l'art. D.112-3 du CMF

• Encadrement de toutes les cartes prépayées, même non anonymes

La loi n°2016-731 du 3 juin 2016 (loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, dite « loi Urvoas ») a pris deux dispositions pour mieux encadrer les cartes de paiement prépayées :

– L'obligation pour les EME de conserver cinq ans les informations clients (art. L.561-12 du CMF) : les émetteurs de ME devront recueillir et conserver pendant 5 ans les informations relatives à l'activation, au chargement et à l'utilisation de la monnaie électronique au moyen d'un support physique.
– Le plafonnement des paramètres d'utilisation des cartes prépayées, même non anonymes (art. L.315-9 du CMF) : le montant maximal stockable sur une carte, les montants de chargement, de remboursement et de retraits en espèces ou en ME anonyme sont plafonnés à des niveaux fixés par décret.

Le décret n°2016-1742 du 15 décembre 2016, transcrit dans l'art. D.315-2 du CMF, a défini ces plafonds. Pour être commercialisé en France, un support physique de monnaie électronique doit désormais répondre aux conditions suivantes :

– Le stockage en ME sur un support physique (plafond d'emport) est limité à 10 000 €.
– Le chargement en espèces ou en ME anonyme, qui impose une prise d'identité au premier euro, est de toute façon limité à 1 000 € par mois calendaire.
– Les retraits en espèces sont limités à 1 000 € par mois.
– Les remboursements de solde en espèces sont également limités à 1 000 € par mois.

• Déclaration des capitaux transférés depuis ou vers l'étranger

Selon l'art. L.152-1 du CMF, repris par l'art. 464 du code des douanes, le porteur de cartes prépayées chargées qui stockerait ainsi sur lui plus de 10 000 € et entrerait ou sortirait d'un pays de l'Union Européenne, serait – au même titre qu'un porteur d'espèces ou d'or physique - soumis aux obligations déclaratives de capitaux auprès de l'administration des douanes.

ANNEXE N°2
LES PRINCIPALES MESURES DE L'ORDONNANCE N°2016-1635 DU 1er DÉCEMBRE 2016, DITE ORDONNANCE DE TRANSPOSITION DE LA 4e DIRECTIVE

L'année 2016 a vu aboutir les travaux de transposition en droit français de la 4ème directive européenne LCB/FT, par l'ordonnance n°2016-1631 du 1er décembre 2016. Cette ordonnance intègre dans le code monétaire et financier plusieurs dispositions qui renforcent le dispositif :

• L'élargissement du périmètre des assujettis (article L.561-2 du CMF)

– Les professions agissant sous statut d'Intermédiaire en Opérations de Banque et de Services de Paiement (IOBSP) sont pleinement assujetties (cf point 3° de l'article L561-2).
– Les agents immobiliers, qui étaient assujettis pour les transactions d'achat/vente de biens, le deviennent également pour les activités de location (cf point 8° du L.561-2).
– La définition des commerçants en biens précieux assujettis au dispositif est précisée (cf point 11° du L.561-2).
Surtout, le droit français a anticipé sur les discussions européennes afin d'intégrer au dispositif LCB/FT de nouveaux acteurs de la transformation digitale :

– Les plateformes de *crowdfunding* proposant des prêts ou des dons (CIP et IFP – Cf point 6° du L.561-2) ;
– Les acteurs des monnaies virtuelles que sont les plates-formes de change entre monnaie réelle et monnaie virtuelle (fiat/crypto), ainsi que les fournisseurs de portefeuilles, également appelés *wallet providers* (cf point 7°bis du L.561-2).

• La consécration d'un dispositif d'évaluation des risques

Chaque déclarant doit, à son niveau, mettre en place une analyse par les risques, en fonction de son activité, de la nature des produits et services qu'il propose, et de la composition de sa clientèle.

Le lien entre l'analyse de risques et les mesures de vigilance est renforcé. Les risques identifiés comme élevés doivent conduire à mettre en place des mesures de vigilance particulières, qu'il s'agisse des produits avec le plafonnement de l'utilisation des cartes prépayées, ou des clients avec la recherche du bénéficiaire effectif.

• L'identification des bénéficiaires effectifs et la mise en place de registres centralisés dédiés

Le registre du commerce et des sociétés devra mettre en évidence les porteurs de parts des personnes morales.

La loi du 6 décembre 2013 avait institué un « registre public des trusts » permettant, selon des modalités renvoyées à un décret, d'avoir librement accès à diverses données personnelles propres aux constituants, aux administrateurs et aux bénéficiaires de trusts (Cf alinea 2 de l'article 1649 AB du CGI).

Selon la décision du Conseil d'Etat n°400913 du 22 juillet 2016, confirmée par la décision du Conseil Constitutionnel n°2016-591 QPC du 21 octobre 2016, ce registre des trusts ne sera accessible qu'aux autorités compétentes. Le deuxième alinea de l'article 1649 AB du CGI a été jugé contraire à la Constitution au regard de la nécessaire protection des libertés individuelles.

L'élargissement de la notion de Personne Politiquement Exposée aux PPE nationales.

• Le renforcement des capacités d'action et d'investigation de Tracfin.

– Extension du droit de communication de Tracfin aux sociétés de location de véhicules, aux Caisses des Règlements Pécuniaires des Avocats (CARPA), et à toute plateforme de crowdfunding qui ne serait pas assujettie.
– Droit d'opposition prolongé à 10 jours, renouvelable une fois, ce qui renforce les possibilités de coopération avec les homologues étrangers afin de stopper l'évasion de fonds frauduleux.
– Amélioration des partenariats entre administrations et élargissement de la liste des destinataires des transmissions de Tracfin (Cour des Comptes et Chambres Régionales des Comptes ; Haute Autorité pour la Transparence de la Vie Publique ; Agence Française Anticorruption ; Service de l'Information Stratégique et de la Sécurité Economique...)
– Protection de la confidentialité des déclarations de soupçon.

Tracfin

Traitement du renseignement et action contre les circuits financiers clandestins

Directeur de publication : Bruno Dalles
10 rue Auguste Blanqui 93186 MONTREUIL - tél. : (33)1 57 53 27 00

www.economie.gouv.fr/tracfin
crf.france@finances.gouv.fr

Maquette : Studio graphique SIRCOM