SECRETARIAT GENERAL

Direction de la lutte contre le blanchiment de capitaux et le financement du terrorisme

Service Coopération et Analyse

A3 – Analyse stratégique

Panorama et analyse des services d'IBAN virtuels offerts en France, sous l'angle de la lutte contre le blanchiment des capitaux et le financement du terrorisme

Avril 2026

PRÉSENTATION DE L'ÉTUDE

L'Autorité de contrôle prudentiel et de résolution (ACPR) a été confrontée, dans le cadre de ses contrôles, aux risques présentés par les identifiants bancaires virtuels (appelés aussi « IBAN virtuels » ou « vIBAN ») et à plusieurs cas d'utilisation risquée de ce type de produits.

Aussi, en mars 2023, la Direction LCB-FT de l'ACPR a mené une étude en s'appuyant sur un questionnaire adressé à 23 établissements[1] (soit un échantillon de 14 établissements de crédit, 5 établissements de monnaie électronique et 4 établissements de paiement, français et étrangers, ayant une présence en France) concernant les « vIBAN ».

Dans le cadre de cette revue, les vIBAN ont été définis comme « la pratique consistant à associer plusieurs codes ayant l'apparence formelle d'un IBAN (vIBAN) à un unique compte de paiement. Les virements émis ou reçus par et depuis un vIBAN sont enregistrés par ce compte maître unique ». Le questionnaire ciblait également des pratiques similaires qui ne seraient pas commercialisées sous le terme de « vIBAN » mais sous d'autres appellations telles que « IBAN-as-a-service ». Le questionnaire s'est concentré sur les services vIBAN impliquant la France, c'est-à-dire lorsque l'une ou plusieurs des conditions suivantes sont remplies :

- le compte maître a un IBAN présentant un code pays français (FR),
- un vIBAN présente un code pays FR,
- une entité française supervisée par l'ACPR propose des vIBAN à sa clientèle (même des vIBAN avec un code pays étranger, et même si la clientèle réside à l'étranger),
- une autre entité du même groupe financier propose des vIBAN à la clientèle française (même si les vIBAN présentent un code pays étranger).

Les résultats préliminaires de cette revue ont été partagés avec plusieurs autorités étrangères homologues, afin de contribuer aux travaux menés par la suite par ces autorités. Ces résultats ont aussi fait l'objet d'échanges avec la Commission Consultative LCB-FT de l'ACPR.

Ce rapport a été enrichi en 2025 de cas d'études réalisés par la cellule de renseignement financier Tracfin, qui permettent d'illustrer les cas d'usage d'IBAN virtuels français et étrangers ainsi que certains risques liés à l'abus de cette pratique dans des schémas financiers d'escroquerie, de fraude aux finances publiques, de blanchiment de capitaux ou encore de contournement de sanctions.

[1] L'un d'entre eux ayant fourni deux questionnaires

SYNTHÈSE

L'enquête montre qu'en juin 2023, 20 participants à l'enquête offraient ou prévoyaient d'offrir des services de vIBAN tels que décrits ci-dessus, qu'ils utilisent ou non la qualification d'IBAN virtuels. Toutefois, pour deux d'entre eux, les services vIBAN reposent uniquement sur l'utilisation de plusieurs comptes à part entière tenus par l'établissement.

Les services d'IBAN virtuels consistent généralement à générer plusieurs IBAN utilisés pour acheminer les paiements vers un compte de paiement unique (parfois appelé compte maître ou compte principal), ce qui fait qu'un compte unique semble avoir plusieurs IBAN.

Les services décrits peuvent viser à répondre à un usage ciblé ou, plus communément, permettre diverses utilisations selon les besoins du client. La grande majorité des cas examinés par l'ACPR relèvent d'usages légitimes, tels que faciliter (i) la réconciliation des paiements (ii) la comptabilité analytique (iii) ou la centralisation de trésorerie au sein des groupes de sociétés.

Toutefois, dans la mesure où certains acteurs proposent des services similaires sans avoir recours aux vIBAN, ces objectifs pourraient être atteints en utilisant un compte de paiement par contrepartie ou par ligne d'activité, avec des règles automatisées (par exemple, des comptes de redirection dont le solde positif est transféré automatiquement vers un autre compte).

Ces services sont fournis depuis une dizaine d'années en France.

La revue met également en lumière la récente apparition de cas d'usage plus risqués des IBAN virtuels tels que (i) la réattribution en cascade de vIBAN et (ii) la fourniture d'IBAN identifiés dans un pays différent du compte maître, qu'il soit français ou non. Ces services vIBAN semblent être utilisés par des réseaux criminels afin de contourner les dispositifs de vigilance, en particulier pour les flux transfrontaliers. En effet, ils opacifient la destination réelle des flux et obèrent la prise en compte du risque géographique par les contreparties. Selon le cas, ils peuvent complexifier les enquêtes des autorités compétentes, les forçant à multiplier les demandes de coopération internationale pour obtenir les informations nécessaires. Ainsi, selon Tracfin, les IBAN virtuels dont le code pays ne correspond pas au lieu de tenue du compte maître présentent des vulnérabilités substantielles en matière de blanchiment, d'escroquerie, de fraude aux finances publiques et de contournement de sanctions.

Fin 2022, les participants à l'étude recensaient :

- 1,7 million de vIBAN actifs (0,7 million pour des clients institutions financières, 0,6 million pour des clients sociétés non financières, 0,4 million pour les clients particuliers) ;
- 400 000 clients utilisant des vIBAN (dont 18 établissements financiers, 18 000 sociétés non financières, les autres étant des particuliers) ;
- 4 milliards d'euros de transactions en un mois (janvier 2023) : 0,6 milliard pour les institutions financières, 3,3 milliards pour les entreprises non financières, 49 millions pour les particuliers.

Le nombre moyen de vIBAN par client varie considérablement : 40 000 par établissement financier, 33 par société non financière et un peu plus d'un pour les particuliers. Il est en revanche difficile de fournir des statistiques par cas d'usage, les établissements financiers n'étant pas nécessairement conscients des usages recherchés par leurs clients et plusieurs d'entre eux pouvant se combiner (rapprochement et centrale de trésorerie, par exemple).

Le présent rapport décrit les utilisations de vIBAN présentant un risque faible (section I), puis les cas d'usage à risque élevé (section II) et l'analyse de l'ACPR sur la réglementation et les mesures d'atténuation pour ces risques (section III).

I - Services d'IBAN virtuels à risque faible

La grande majorité des cas examinés par l'ACPR portent sur des utilisations légitimes présentant un risque faible, notamment pour faciliter :

(i) **la réconciliation des paiements** (affectation des paiements aux contreparties, chaque payeur se voyant attribuer un IBAN différent),
(ii) **la comptabilité analytique** (différents IBAN utilisés par les différentes lignes métier) ;
(iii) **la gestion de trésorerie** par des « centrales de trésorerie » qui opèrent des transactions financières pour plusieurs filiales au sein de groupes de sociétés.

Les organismes financiers considèrent que l'utilisation de vIBAN peut faciliter le suivi des flux financiers, en fournissant au client une vue analytique de ses transactions bancaires, dès lors que chaque flux bancaire peut être catégorisé dès son enregistrement. Les vIBAN apparaissent comme un moyen fiable de rapprocher automatiquement les flux, dans la mesure où le numéro de compte est reporté avec précision dans les messages de paiement, y compris en cas de transfert transfrontalier, tandis que les informations accompagnant la transmission de fonds (telles que les références de facture) peuvent être perdues.

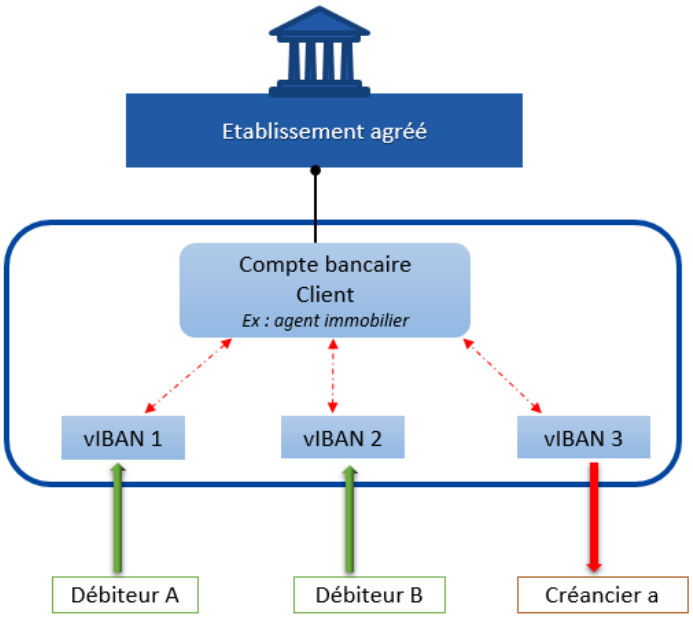
Selon les organismes financiers, l'utilisation d'un IBAN virtuel peut également améliorer la traçabilité des transactions internes, tant pour le client que pour l'établissement financier teneur du compte de paiement. Les procédures internes de surveillance des comptes peuvent ainsi gagner en rapidité et en efficacité, en permettant de conserver une vision consolidée des transactions du client sur le compte maître.

Les participants considèrent que l'utilisation de vIBAN contribue à réduire le risque de fraude, en évitant la communication de l'IBAN du compte maître aux tiers et en limitant les flux sortants depuis les vIBAN. Le même résultat peut cependant être obtenu avec le recours à deux comptes classiques.

Cas 1 : Réconciliation des flux

Un IBAN virtuel différent est communiqué par le client de l'organisme financier à chacun de ses débiteurs (c'est-à-dire, à chaque personne dont le client attend un paiement).

En conséquence, la réception d'un paiement sur un vIBAN individualisé permet d'identifier automatiquement l'émetteur du transfert. Le rapprochement entre flux financiers et facturation n'est plus subordonné à la mention par les contreparties d'un libellé de virement (comme la mention d'une référence de facture, d'un nom) ou à la vérification du nom du donneur d'ordre. Cela facilite, par exemple, l'identification des factures restées impayées. La version révisée du règlement européen sur la transparence des fonds pourrait toutefois restreindre cette utilité des IBAN virtuels, dès lors qu'elle impose dans chaque flux de paiement la mention des identifiants d'entités légales (par exemple, le « *Legal Entity Identifier* ») pour en identifier les parties.



Cas 1 - Réconciliation des flux

A la date de l'étude, les trois quarts des participants proposaient ou envisageaient de fournir des services d'IBAN virtuels à des fins de réconciliation. Un établissement proposait un service de rapprochement similaire reposant sur la fourniture de plusieurs comptes de paiement.

Selon les résultats de l'enquête, les principaux utilisateurs de ces services sont de grands remettants procédant à de nombreux encaissements (tels que les bailleurs immobiliers ou les places de marché). Les vIBAN sont principalement utilisés pour distinguer les payeurs et ségréger les virements entrants.

Illustration n°1 : Utilisation d'IBAN virtuels pour faciliter la réconciliation des flux par un casino en ligne ou par un prestataire de services sur crypto-actifs numériques[2] (PSCA)

Un casino en ligne étranger peut disposer d'un compte tenu par un établissement de crédit (EC) ou prestataire de services de paiement (PSP), et de plusieurs IBAN virtuels associés à ce compte. Il peut attitrer chacun de ces IBAN virtuels à l'un de ses clients. Dès lors, il peut proposer auxdits clients de créditer automatiquement leur compte de jeu en ligne *via* un virement effectué à destination de l'IBAN virtuel qui leur est attitré. À réception des fonds sur son propre compte, le casino en ligne crédite le compte- joueur de la somme transférée.

Un PSCA a un compte tenu par un EC/PSP, auquel sont associés des IBAN virtuels. Il les attitre à ses propres clients. Dès qu'il reçoit sur son compte un virement par l'intermédiaire de l'un de ces IBAN virtuels, il crédite la contre-valeur en crypto-actifs sur le *custodial wallet* du client auquel l'IBAN virtuel a été attitré.

2e cas : Gestion analytique des flux bancaires

Un IBAN virtuel est attribué à une sous-catégorie d'opérations effectuées par le client agissant pour son propre compte. Ce type de services est proposé à la place de sous-comptes, afin de fournir une

[2] A la date de l'étude, les cas relevés concernaient les prestataires de services sur actifs numériques (PSAN), catégorie issue de la loi PACTE du 22 mai 2019. Toutefois, ils concernent de manière similaire la catégorie des prestataires de services sur crypto-actifs (PSCA) créée par le Règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs (« règlement MICA »),

vision analytique des transferts, en les rattachant à différentes catégories librement définies par le client, tout en simplifiant la structure du compte.

Il permet de référencer un ensemble de flux entrants et sortants en leur attribuant un IBAN spécifique. Par exemple, les IBAN virtuels peuvent être utilisés pour discriminer :

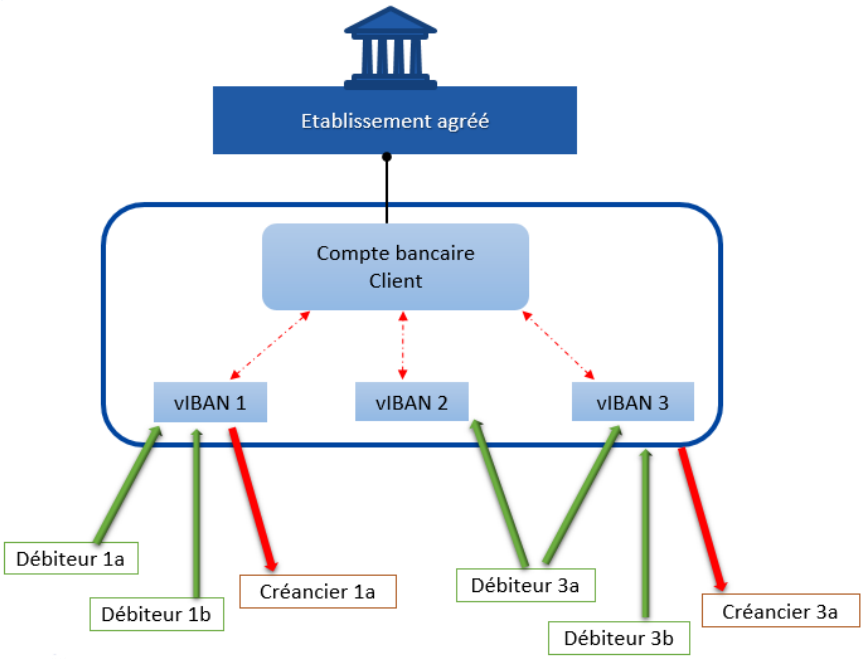
- une partie de l'activité (branche d'activité, ligne de production...)
- une catégorie de dépenses (impôts, salaires, frais généraux)
- un type de clientèle (clients A, clients B) ;
- un régime de taxation (opérations bénéficiant d'une exonération de TVA, ou d'un taux de TVA spécifique) ;
- flux dans certaines devises.

Ce cas d'usage des vIBAN est principalement constaté pour des sociétés non financières. Dans ce type de services, tous les transferts sont reçus ou émis par le titulaire du compte de paiement pour son propre compte.

Illustration n° 2 : Utilisation d'IBAN virtuels pour faciliter la gestion analytique des flux par les CARPA

Les CARPA utilisent par exemple ce type de services afin de créer des comptes virtuels par avocat et par affaire, afin de faciliter grandement pour eux l'ouverture de compte et le suivi des transactions.

Ce service permet au client de configurer des règles de gestion automatique pour un groupe d'opérations (par exemple, appliquer un taux de TVA à une catégorie d'opérations) ou de classer les flux en fonction de leur devise.



Cas 2 - comptabilité analytique

L'usage des IBAN virtuels pour faciliter la réconciliation des paiements (cas 1) et la comptabilité analytique (cas 2) par le client, présentent un niveau de risque similaire.

➢ Un risque global faible : complexité accrue de la vigilance des transactions pour les tiers

Ces cas d'utilisation présentent un risque global faible, en dépit du fait qu'ils complexifient le suivi des transactions pour les tiers (détection plus difficile de schémas « many-to-one », où plusieurs paiements apparaissant aller vers des comptes différents sont en réalité destinés au même compte).

Illustration n°3 - Risques liés au contournement des mécanismes de détection du fractionnement

Un compte peut avoir un grand nombre d'IBAN virtuels. Afin de faire en sorte qu'un virement important vers un compte ne soit pas détecté par les systèmes de vigilance automatique de la banque émettrice, ce virement pourrait être fractionné en plusieurs opérations à destination de plusieurs IBAN virtuels associés au compte destinataire (plusieurs opérations à destination d'un même IBAN seraient plus aisément détectées). Un tel fonctionnement pourra cependant déclencher d'autres scénarios d'alerte.

Certains participants ont indiqué autoriser également l'utilisation d'IBAN virtuels pour émettre des paiements : dans ce cas, l'IBAN virtuel apparaît dans le message de paiement comme compte émetteur de l'opération. **Il est important dans ce cas que le prestataire de services de paiement respecte la réglementation sur la transparence des transferts de fonds, qui exige des établissements financiers initiateurs de virements qu'ils vérifient l'exactitude des informations relatives au donneur d'ordre dans les messages de paiement, et notamment que le numéro de compte soit bien celui du compte d'où le paiement est effectué.**

Illustration n° 4 - Risques liés à des messages de paiement incomplets pour les tiers

Les IBAN virtuels peuvent dissimuler la destination et l'utilisation effective des fonds. Comme dans l'illustration n°1, un PSP A met des IBAN virtuels à disposition d'un PSCA B qui en attribue un à chacun de ses clients. L'ACPR a pu constater, dans certains cas, que des relevés d'identité bancaire associaient un tel IBAN virtuel émis par le PSP A, à un client C du PSCA B, donnant l'apparence que le vIBAN correspond à un compte dont le titulaire serait C. Ce système se traduit par des messages de paiement où le nom du bénéficiaire est C, le nom du client final. De ce fait, la banque émettrice pourra connaître le destinataire final des fonds. Cependant, ce schéma a l'inconvénient de dissimuler l'objectif de l'opération car l'IBAN du destinataire ressort comme le client C. En effet, si un virement est émis à destination d'un IBAN au nom du PSCA B, avec une référence appropriée, la banque émettrice pourrait supposer qu'il s'agit d'un achat de crypto-actifs, et le prendre en compte dans sa vigilance. En revanche, si le virement est émis à destination d'un IBAN virtuel au nom d'un particulier, par exemple de son client, elle pourra simplement supposer qu'il est multi-bancarisé.

La question de telles chaînes hybrides, où, économiquement, un paiement en monnaie fiat aboutit sur un portefeuille de crypto actifs, pourra faire l'objet de discussions au GAFI dans le cadre des futures lignes directrices sur l'application de la recommandation 16 du GAFI. En l'état actuel du droit, le message de paiement devrait faire apparaître le nom du titulaire du compte bénéficiaire, à savoir le PSCA B.

En outre, lorsque les vIBAN ne figurent pas dans les registres des comptes bancaires nationaux, les autorités ne peuvent pas accéder immédiatement aux informations utiles, telles que le nom du bénéficiaire vérifié, la date d'ouverture du compte et les bénéficiaires effectifs, qui doivent figurer dans ces registres en application de la 5ème directive anti-blanchiment.

➢ Mesures d'atténuation possibles

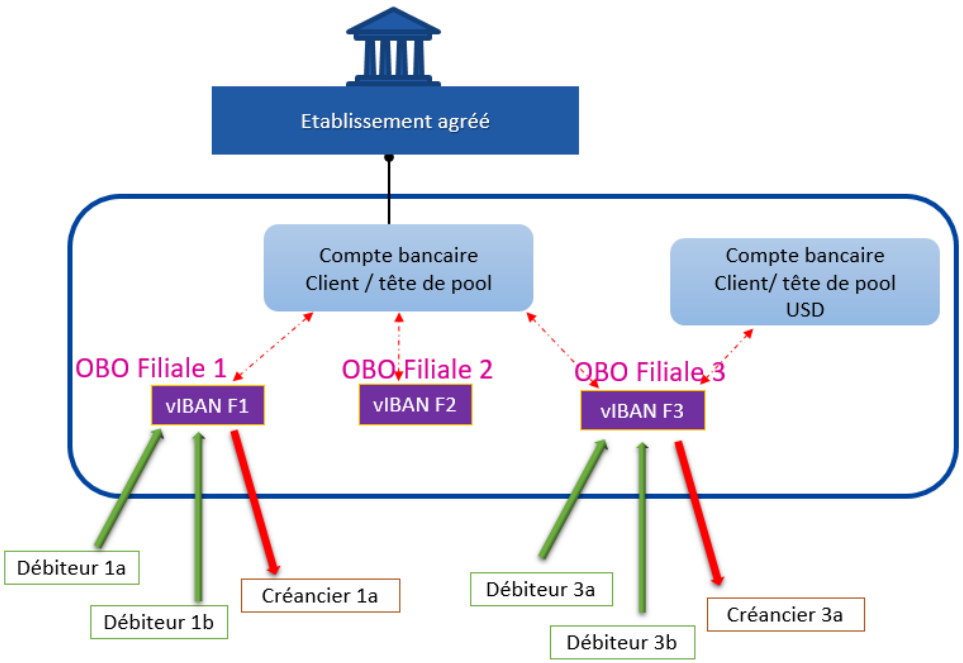
Ce risque peut être atténué comme décrit ci-dessous :

- L'obligation de mentionner l'identifiant d'entité juridique (tel le numéro IEJ ou LEI en anglais), tel que visé dans la version révisée du règlement sur les transferts de fonds[3], pourrait faciliter l'identification des schémas « many-to-one », mais uniquement pour les personnes morales.
- Les services d'IBAN virtuels pourraient être limités aux clients qui en ont un besoin clairement justifié, en excluant les clients exposés à un risque élevé d'utilisation de ce service à des fins de BC-FT.
- La déclaration des vIBAN aux registres de comptes bancaires nationaux a été rendue obligatoire par la 6ème directive anti-blanchiment qui entrera en application en 2027.
- La mise en œuvre de la révision de la recommandation nº 16 du GAFI devrait également atténuer les risques. En effet, elle impose aux établissements bénéficiaires de mettre en œuvre des mécanismes visant à vérifier que les informations sur les bénéficiaires contenues dans les messages de paiement correspondent à celles vérifiées dans leurs registres.
- L'utilisation du champ « bénéficiaire ultime », en complément du champ bénéficiaire, dans les messages qui le permettent (ISO 20022), pourrait faciliter l'identification du client final.

Cas n° 3 : Centrales de paiement au sein de groupes de sociétés

Un quart des personnes interrogées déclarent proposer depuis plusieurs années des services vIBAN visant à faciliter la gestion des centrales de paiement au sein des groupes de sociétés.

Un vIBAN est alloué à chaque filiale du groupe, et rattaché au compte ouvert au nom de l'entité qui se voit confier la centralisation de la trésorerie. Le service permet au client de faciliter la gestion des paiements qu'il reçoit ou émet pour le compte des filiales qu'il contrôle, tout en conservant une visibilité immédiate par filiale.



Cas 3 - Centrales de paiement

[3] Règlement (UE) 2023/1113 du 31 mai 2023.

Illustration n° 5 - Utilisation d'IBAN virtuels à des fins de centralisation des paiements

Dans le cadre d'une « payment factory » ou « usine à paiements », le client de l'EC/PSP est généralement un groupe qui souhaite centraliser l'ensemble des opérations de ses filiales sur un seul compte « maître » : à chaque filiale est attribué un IBAN virtuel, dont les opérations sont enregistrées sur le compte centralisateur. On parle de fonctionnalités « COBO » (collecte pour compte de tiers) ou « POBO » (paiement pour compte de tiers). Ce modèle permettrait de réduire les coûts de tenue et de création de compte (l'alternative étant d'ouvrir un compte « réel » par filiale).

L'utilisation d'IBAN virtuels pour les besoins de centrales de paiement est présentée comme un moyen de réduire les frais de tenue de compte. Certains établissements pratiquent en effet des frais réduits, dès lors que ces comptes ne présentent pas de solde et n'engendrent pas les frais de gestion de comptes habituels. Il convient toutefois de noter que des réductions de frais peuvent être également pratiquées par les établissements, en cas de centrales de paiement fonctionnant avec des comptes séparés. **Cet avantage semble donc relever davantage d'une politique tarifaire de l'établissement que d'une véritable économie liée à l'utilisation de vIBAN.**

Ces services peuvent être combinés avec d'autres services de vIBAN visant à faciliter la réconciliation comptable ou la gestion analytique des flux, évoqués *supra*.

➢ Un risque modéré à condition que des mesures d'atténuation soient appliquées

Ce troisième cas d'usage présente un risque modéré, à l'exception des aspects suivants :

- L'établissement financier qui émet des vIBAN n'a pas d'obligation de collecter des éléments de connaissance client à l'égard des filiales, en l'absence de relation d'affaires avec elles. Toutefois, cette absence de collecte d'informations ne peut être admise qu'à la condition que la tête de la centrale de trésorerie soit autorisée à recevoir des fonds pour le compte de tiers et que ces comptes ne sont pas directement détenus ou utilisés par ces tiers (les filiales). L'identification des entités du groupe concernées paraît néanmoins nécessaire afin d'être en mesure de connaître les bénéficiaires effectifs des opérations, au titre de l'article L. 561-2-2 2° du code monétaire et financier.
- Les fonds concernés pourraient être indûment affectés à la filiale ou à l'entité centralisatrice.
- L'utilisation de vIBAN peut masquer le risque géographique si la centrale de paiement inclut des sociétés sises dans plusieurs pays.

Certains participants ont mentionné pratiquer certaines mesures d'atténuation des risques :

- Certains établissements limitent les offres d'IBAN virtuels aux groupes de sociétés afin d'éviter que leur client encoure la qualification d'exercice illégal d'activité de fourniture de services de paiement, à défaut des agréments nécessaires.
- L'accès aux services de centralisation de trésorerie peut être réservé aux groupes de sociétés et subordonné à des conditions de pourcentage de détention des filiales ou de solvabilité.
- Les institutions financières mettent couramment en place des procédures permettant de vérifier les liens capitalistes et la réalité du groupe de sociétés, voire en collectant une certaine forme de connaissance client à l'égard des filiales.

Il est nécessaire de distinguer avec attention si les vIBAN sont utilisés par l'entité centralisatrice de trésorerie pour le compte de filiales, ou directement par des filiales comme s'il s'agissait de leurs propres comptes. Dans ce dernier cas, l'utilisation de vIBAN peut entraîner une violation des exigences en matière de connaissance client et du règlement sur le transfert de fonds. Les exigences relatives

aux bénéficiaires effectifs semblent insuffisantes pour atténuer ces risques, du fait qu'elles concernent les personnes physiques (et non un réseau de filiales) et ne requièrent pas le même niveau de vérification.

* *
*

Analyse de l'ACPR sur ces trois cas d'usage

En France, ces trois premiers cas d'utilisation de vIBAN sont admis dès lors qu'ils sont analysés comme la fourniture de plusieurs comptes fusionnés dans un compte maître, ce dernier disposant d'un IBAN et enregistrant l'ensemble des opérations exécutées sur les comptes fusionnés. L'ACPR requiert que ces comptes fusionnés présentent des caractéristiques homogènes et soient détenus par le même établissement et au nom du même client. À noter que l'étude de l'ACPR montre que les vIBAN ne sont pas toujours considérés par les institutions financières comme des comptes devant être déclarés dans le registre national des comptes bancaires.

* *
*

II - Services d'IBAN virtuels à risque élevé

Du point de vue de la LBC/FT, deux catégories de services de vIBAN apparaissent particulièrement risquées :

- Cas nº 4 : réattribution en cascade de vIBAN
- Cas n°5 : fourniture de vIBAN avec un code de pays différent du pays dans lequel le compte est tenu.

Cas 4 : Réattribution en cascade d'IBAN virtuels

Certains établissements proposent des services de vIBAN destinés à faciliter l'encaissement de paiements pour le compte des clients de leurs clients, dans le cadre d'une relation contractuelle n'impliquant pas l'établissement teneur du compte[4]. Contrairement au premier cas d'usage sus-décrit, les conditions d'utilisation des IBAN virtuels permettent au titulaire du compte (PSP principalement) de réattribuer les vIBAN à leurs propres clients (offre « en cascade »). Les vIBAN distribués au titulaire du compte principal paraissent en effet dans certains cas être réattribués par des PSP successifs, sans limite du nombre de réattributions consécutives. Le nombre d'intermédiaires dans le circuit financier peut être élevé.

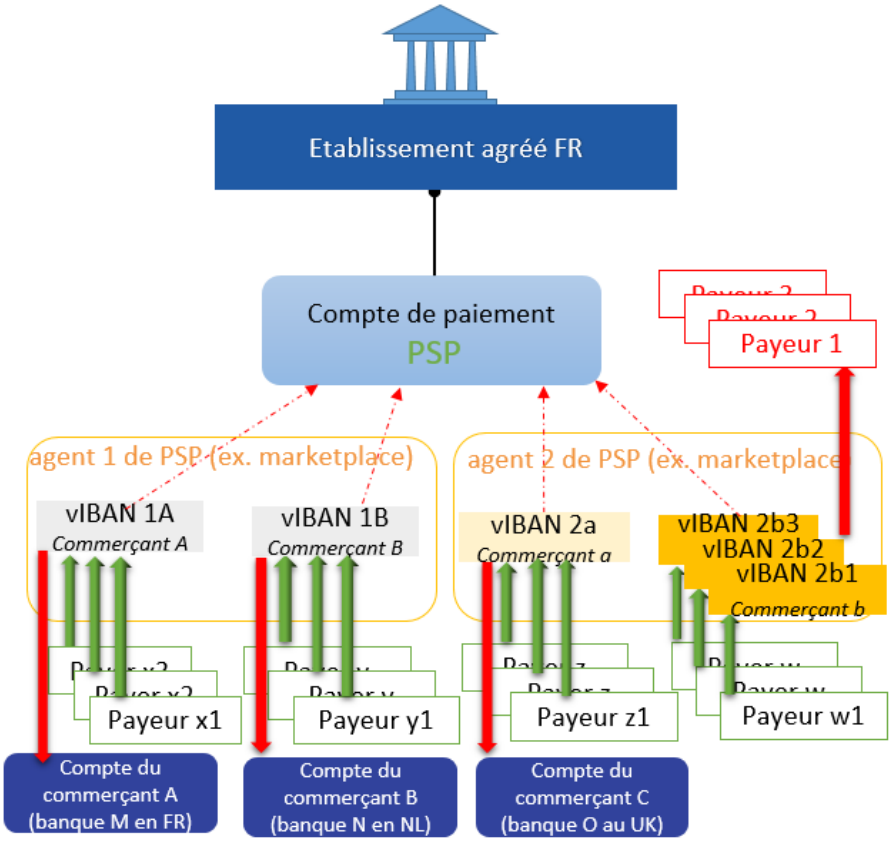
L'ACPR n'a que rarement rencontré de tels cas en France, car les établissements de paiement et de monnaie électronique français reçoivent leurs propres codes interbancaires, et leurs IBAN font apparaître ce code pour les identifier.

Un cas d'utilisation a notamment été identifié chez un établissement déclarant un très grand nombre d'utilisateurs de vIBAN.

[4] Ce service est distinct d'autres qui peuvent par ailleurs être proposés, comme l'accès aux infrastructures de paiement ou le compte de cantonnement.

La fonctionnalité de réattribution pourrait principalement être utilisée par des PSP tenant les comptes de places de marché en relation avec de nombreux commerçants (qui peuvent parfois eux-mêmes être des agents de PSP). Elle permet en outre à des plateformes de financement participatif de collecter des paiements pour plusieurs porteurs de projets.

Dans le schéma suivant, la chaîne comprend trois niveaux : un EC émet pour le compte d'un client PSP une série de vIBAN rattachés au compte de ce PSP ; ce PSP propose ces vIBAN à ses clients, des marketplaces dans l'illustration suivante.



Cas 4 – facilitation des encaissements pour compte de tiers, avec réattribution en cascade

Si un PSP affecte un vIBAN à l'un de ses clients directs, pour ses propres besoins de réconciliation, le niveau de risque apparaît aussi faible que pour les autres services de réconciliation examinés dans les premiers cas d'usage susmentionnés. Néanmoins, sur le schéma ci-dessus, **lorsqu'un vIBAN est attribué non pas au propre client du PSP (marketplace 1) mais à un client de celui-ci (un commerçant A) pour faciliter l'encaissement des paiements émis par des payeurs X1, X2 et X3 destinés au commerçant A, les risques sont beaucoup plus élevés.**

Illustration n° 6 – Réattribution en cascade d'IBAN virtuels

Dans l'exemple ci-dessus, l'établissement agréé FR n'a pas de relation contractuelle avec les *market places* 1 et 2 ni avec les commerçants A, B, a et b, mais effectue des diligences sur son client, le PSP. Le PSP, qui utilise ses comptes auprès de l'établissement agréé FR pour traiter les paiements reçus par ses clients, est responsable des diligences de connaissance sur ces relations d'affaires. Les situations varient cependant d'une place de marché à l'autre :

> certaines peuvent être le fournisseur effectif du bien ou du service vendu et recevoir le paiement dans leur patrimoine (le commerçant A peut n'être qu'un fournisseur de la marketplace). Dans ce cas, le client du PSP serait la marketplace.

> d'autres ne font que rapprocher le commerçant de ses clients. Dans ce cas, les commerçants, seraient également clients du PSP.

En pratique, le PSP n'a pas toujours correctement identifié le véritable objet du paiement reçu et n'est pas en mesure d'exercer une vigilance effective sur les flux (notamment pour vérifier si les flux sont cohérents avec sa connaissance de la relation d'affaires).

1) Risque de complexification de la vigilance

- **Manque d'informations sur l'utilisateur final des vIBAN :** lorsque le client est un PSP qui utilise des vIBAN pour exécuter les opérations de ses propres clients, l'établissement émetteur des vIBAN n'est pas en relation d'affaires avec les utilisateurs finaux des vIBAN. Par conséquent, l'établissement financier émetteur collecte uniquement les éléments de connaissance client à l'égard du PSP, et aucun à l'égard de l'utilisateur réel des vIBAN.

  La segmentation du dispositif de vigilance entre l'établissement teneur du compte maître et le titulaire du compte peut aggraver le niveau de risque. Il en est de même lorsqu'un client final se voit attribuer plusieurs vIBAN, ce qui aboutit à fractionner son activité financière entre plusieurs identifiants bancaires.

Illustration n° 7 – Risques liés à l'absence de relation d'affaires directe avec l'utilisateur final d'IBAN virtuels réattribués en cascade

Dans cette situation, l'établissement A (qui est désigné par le code banque et le code pays de l'IBAN virtuel) peut, selon ses politiques internes et ses accords avec son client le PSP B (qui attitre l'IBAN virtuel à son propre client), ne disposer que d'informations parcellaires sur le client final.

Aussi l'établissement A n'a accès ni au compte du client final (il ne peut voir que les transactions transitant par l'IBAN virtuel, et n'a ainsi qu'une vision parcellaire du fonctionnement des opérations de ce client avec le PSP), ni au client final pour demander des clarifications et documents supplémentaires.

Ainsi, l'établissement A repose sur le PSP B en termes de :

- L'exercice de la vigilance constante sur les opérations : l'établissement A ne dispose pas du contexte nécessaire pour identifier correctement les opérations suspectes.
- Réponse aux questions des cellules de renseignement financier et autres autorités compétentes sur les vIBAN qu'il met à disposition du PSP B.

  Certains établissements ont mis en place, à titre de bonne pratique, des procédures permettant de collecter une connaissance client allégée des clients finaux.

- **Un effet de fragmentation sur le comportement financier** : l'utilisation de plusieurs vIBAN pour un seul utilisateur final peut compliquer l'exercice de la vigilance sur les opérations. Dans de tels cas, il est nécessaire que l'établissement teneur de compte s'assure que les procédures de vigilance appliquées par le PSP titulaire du compte à l'égard de ses propres clients

permettent d'exercer une vigilance sur l'activité transactionnelle de chaque marketplace ou commerçant (permettant notamment de comparer l'ensemble des opérations sur les différents vIBAN concernés avec la connaissance du client).

En raison de la structure similaire des IBAN et des vIBAN, les établissements ne peuvent pas détecter la présence d'un vIBAN lorsqu'ils reçoivent un flux d'un vIBAN externe ou lorsqu'ils émettent un flux sortant à destination d'un vIBAN externe. Le dispositif de surveillance des transactions ne peut donc pas tenir compte de la nature de vIBAN, car il n'existe **aucune référence normalisée pour les vIBAN dans les messages de paiement**.

Le dispositif de vigilance pourrait par exemple être mis en échec en permettant à un client de contourner les seuils de validation manuelle des transactions par un **fractionnement des transactions entre plusieurs IBAN virtuels**, alors que la réalisation des transactions cumulées à l'aide d'un seul IBAN aurait déclenché le passage en validation manuelle.

La plupart des participants à l'enquête n'appliquent pas de mesures de vigilance spécifiques aux transactions enregistrées par un vIBAN, estimant que le suivi des transactions effectué sur le compte principal suffit pour couvrir l'ensemble des transactions. Toutefois, les réponses montrent que certains établissements n'ont pas été en mesure de fournir des chiffres sur les vIBAN actifs.

2) Risque lié à l'utilisation de vIBAN à titre de compte de paiement

L'utilisation d'IBAN virtuels a pour effet de masquer le destinataire final des flux, quand il n'est pas le titulaire du compte maître. Par exemple, un client d'un commerçant qui initie un paiement vers celui-ci peut ignorer que les flux sont reçus sur un compte dont le commerçant n'est pas titulaire.

- **Encaissement de fonds pour le compte de tiers, sans agrément** : les services d'IBAN virtuel sont susceptibles de faciliter l'infraction d'exercice illégal d'activité de fourniture de services de paiement définis à l'article L. 314-1 du Code monétaire et financier, en facilitant l'encaissement de fonds pour le compte d'un tiers, sans être dûment agréé ou mandaté comme agent.

  Certains établissements estiment que le risque de fraude est faible, dès lors qu'ils limitent l'utilisation des vIBAN à la réception de flux ou ne proposent les services de vIBAN qu'aux entités juridiques enregistrées en tant qu'agents de PSP, ou au contraire en excluent tous les PSP. Un autre établissement interdit expressément à ses clients PSP de distribuer des vIBAN à titre de comptes de paiement. Certains établissements contrôlent l'utilisation abusive du vIBAN qu'ils émettent : par exemple, un établissement a émis une déclaration de soupçon en janvier 2023 sur une telle pratique, l'un de ses agents ayant utilisé des vIBAN rattachés à son propre compte de paiement pour se faire passer pour un PSP et faire croire à ses victimes qu'il pouvait créer des comptes.

Illustration n° 8 - Facilitation de l'exercice illégal d'une profession financière

Soit une entreprise A disposant d'un compte offrant la possibilité de créer un nombre infini d'IBAN virtuels associés. Ces IBAN virtuels peuvent avoir une apparence et des fonctionnalités presque identiques à des coordonnées bancaires - aussi A peut proposer à ses clients des services de paiement, avec une apparence de légitimité, sans agrément.

- **Utilisation d'un vIBAN comme un véritable compte de paiement par des tiers** : le principal risque est qu'un vIBAN puisse être utilisé par un tiers comme un véritable compte de paiement, sans être soumis aux vigilances appropriées en matière de lutte contre le BC/FT. Le vIBAN serait alors l'équivalent d'un compte anonyme.
  Les risques sont particulièrement élevés lorsque les services associés au vIBAN ressemblent à ceux de comptes « normaux », par exemple lorsque l'utilisateur final peut, en plus de recevoir des paiements :

- émettre des documents qui associent le vIBAN à des tiers autres que le titulaire du compte vérifié (en France : « relevé d'identité bancaire ») ;
- avoir accès à l'équivalent d'un relevé de compte vIBAN, ce qui peut être facilité par des API permettant, par exemple, à une place de marché d'offrir à ses clients commerçants l'accès à des informations sur les paiements qu'elle a reçus pour leur compte (la confusion avec un compte autonome est particulièrement grande si l'IBAN virtuel peut avoir un solde) ;
- générer des paiements au profit de contreparties de son choix, notamment grâce à la pratique d'interfaces programmables, quel que soit le numéro de compte apparaissant comme émetteur (la confusion avec un compte à part entière sera encore plus grande si l'IBAN virtuel apparaît comme émetteur).

Illustration n° 9 - Risques liés à l'utilisation d'IBAN virtuels pour émettre des flux

Soit un IBAN virtuel associé au compte omnibus d'un PSP B tenu auprès d'un EC A. Le PSP B attitre l'IBAN virtuel au compte de l'un de ses propres clients, C. Le client C utilise son IBAN virtuel pour transférer des fonds vers un compte tiers. Son compte chez le PSP B est débité en conséquence. Comme le compte de clientèle débité est celui de C auprès de B, c'est le nom du donneur d'ordre initial (C) qui devrait apparaître sur le message de paiement, respectant ainsi la travel rule : dans ce cas, le risque de BC-FT est limité. Si c'est par contre le nom du PSP B qui apparaît, le risque est élevé, car la banque contrepartie n'a pas de visibilité sur l'origine du flux.

De nombreuses sociétés interrogées offrent à leurs clients la capacité de créer, supprimer ou désactiver des vIBAN sans aucune intervention de l'établissement financier émetteur du vIBAN, et avec un suivi limité de l'utilisation réelle de ces vIBAN.

Les mesures d'atténuation de ces risques peuvent inclure de :

- considérer les vIBAN comme des comptes de paiement à part entière et soumettre leurs titulaires aux obligations de vigilance LCB-FT par leur PSP ; l'**ACPR considère qu'un grand nombre des « vIBAN » sont en réalité des comptes de paiement autonomes** ;
- S'assurer que les paiements sont destinés au titulaire du compte principal lui-même (place de marché ou agent immobilier), ou que ce tiers est habilité à percevoir des paiements pour compte de tiers ;
- Limiter les paiements sortants aux autres comptes de l'utilisateur du vIBAN (en excluant les paiements au profit de tiers) : par exemple, dans les cas où des vIBAN sont attribués à chaque marchand d'une place de marché, les paiements sortants ne pourraient être faits que vers le compte de chaque marchand auprès d'un autre prestataire de services de paiement.

* *
*

L'ACPR analyse les cas de réattribution des IBAN virtuels en cascade comme particulièrement risqués.

Cas 5 : Fourniture de vIBAN dont le code pays diffère du pays de tenue du compte principal

Certains services d'IBAN virtuels permettent d'opérer des flux qui sont enregistrés *in fine* sur un compte principal détenu dans un autre pays. Par conséquent, les vIBAN ont un code pays différent de celui du compte de paiement final.

Certains services qualifiés de « services d'IBAN » consistent à permettre aux clients d'avoir des comptes avec différents codes de pays, tout en considérant que les comptes sont tous tenus dans le même pays. Les vIBAN peuvent être émis soit grâce à un partenariat avec un établissement partenaire local (cas 5a), soit grâce à une succursale locale du même établissement (cas 5b).

Les établissements concernés considèrent que ces services réduisent les frais de gestion des comptes, ceux applicables aux IBAN virtuels étant inférieurs à ceux de la fourniture de sous-comptes. Les vIBAN permettent également d'offrir des options de paiement locales, en devise locale, dans différents pays, réduisant ainsi les frais de change. De cette manière, les transactions peuvent être effectuées plus rapidement et à des taux de change plus faibles dans les pays concernés, en étant traitées par les réseaux de paiement locaux. Enfin, les IBAN locaux peuvent être plus facilement acceptés par les contreparties et permettent d'éviter toute discrimination en fonction du pays d'émission de l'IBAN.

Contrairement aux autres services vIBAN, le nombre de vIBAN fournis est généralement d'un par client et par code pays. La création et l'utilisation de vIBAN reposent généralement sur un processus automatisé sans intervention de l'établissement financier.

Illustration n° 10 – Utilisation d'IBAN virtuels « multi-pays » par des commerçants exerçant leur activité dans plusieurs pays

Un commerçant du pays tiers B souhaite vendre ses produits efficacement au sein de l'Union européenne, mais veut éviter de subir les frais et la complexité d'une relation bancaire auprès d'une banque européenne. Il choisit de passer par un PSP du pays B qui offre des IBAN virtuels d'un pays européen A ; code pays « AA ». Ce PSP n'est pas établi dans le pays « A », mais a ouvert un compte omnibus auprès d'une banque du pays « A », associé à des IBAN virtuels « AA ». Le PSP attribue au commerçant du pays B un de ces IBAN virtuels. Les fonds virés par les clients du commerçant vers cet IBAN virtuel sont versés sur le compte omnibus du PSP dans le pays A. Le PSP crédite en conséquence le compte de son client dans le pays B, voire permet au vIBAN AA de conserver un solde dans la monnaie de AA.

L'enquête met en évidence deux modèles de vIBAN ou « services d'IBAN » qui dissocient le code pays du vIBAN du lieu où les fonds sont détenus. Les risques inhérents à ces deux modèles sont analysés ci-après. Si les cas d'usage sont limités à un nombre très restreint d'établissements, ceux-ci reçoivent environ 20 % de la valeur des virements frauduleux en France (évaluée à partir des demandes de rappels de virements déclarées à l'Observatoire de la Sécurité des Moyens de Paiement).

5.a - Fourniture d'un vIBAN étranger lié à un compte français

Le premier modèle consistait, pour la succursale française d'un établissement financier de l'UE, à fournir à ses clients un compte français ainsi que des IBAN supplémentaires de code pays étranger, par exemple pour les devises autres que l'euro. Les opérations de paiement étaient initiées directement

par le client français à partir de cet IBAN virtuel vers des bénéficiaires externes, les références de ce vIBAN étant mentionnées dans les virements et les relevés de comptes.

Chaque vIBAN faisait référence au code interbancaire de deux établissements partenaires étrangers agréés dans un autre État membre de l'UE. Ces partenaires mettaient à disposition de l'établissement français un compte de paiement (appelé ci-après compte omnibus ou « pool account »). Les fonds émis à destination des vIBAN sont enregistrés sur ces comptes omnibus. Les relevés des comptes de la succursale française présentaient l'apparence de comptes à part entière, avec des numéros de comptes et des soldes différents.

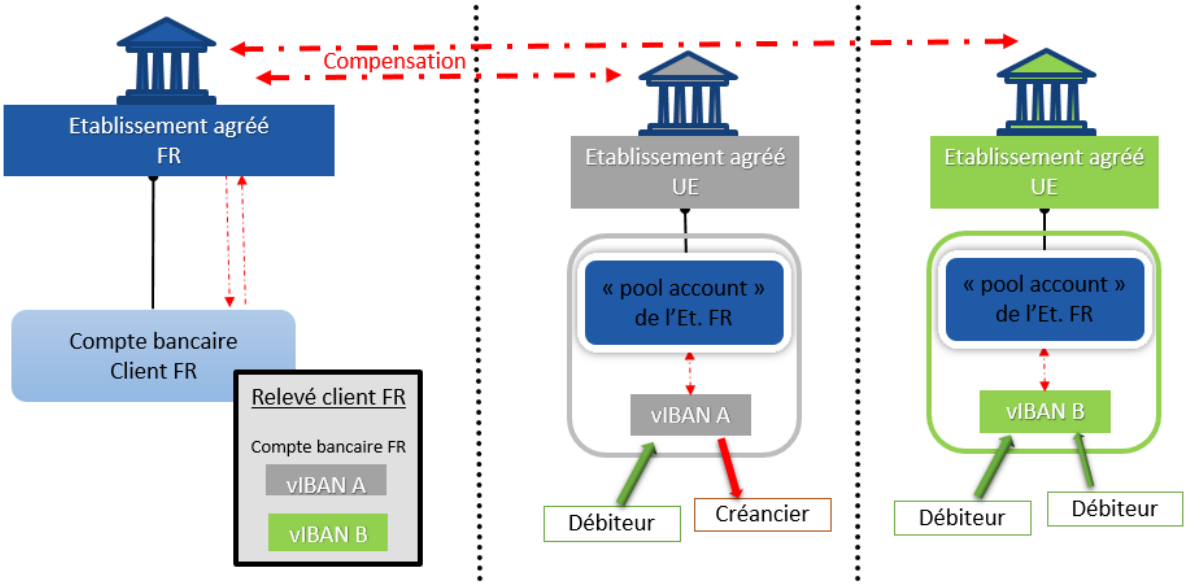
Illustration n° 11 – Fourniture de portefeuilles multidevises sous la forme d'IBAN virtuels

Les fournisseurs d'IBAN virtuels multi-pays associent souvent cette offre à la possibilité de gérer plusieurs devises. Il y aura ainsi autant d'IBAN virtuels (ou autres identifiants de comptes pour les pays n'utilisant pas l'IBAN) que de devises : par exemple, un IBAN PL pour payer et être payé en zlotys, un IBAN GB pour les livres sterling, un IBAN BE pour les euros. Ces produits multidevises offrent généralement des services de change entre les différentes devises couvertes. Ces produits permettent par exemple de maîtriser le risque de change : une entreprise ou un particulier, qui sait qu'il aura à effectuer des paiements dans une certaine devise, peut convertir à l'avance et conserver les sommes dans la devise en question. Ils permettent aussi d'éviter des frais de change quand les paiements reçus dans une devise étrangère s'accompagnent aussi de paiements émis dans cette même devise. Cependant, ils peuvent aussi donner l'apparence d'un paiement domestique à un paiement international, et contourner les réglementations mettant en œuvre la recommandation 16 du GAFI sur la transparence des transferts de fonds. C'est pourquoi le GAFI a inclus, dans la révision de cette recommandation parue en juin 2025, un nouveau paragraphe 7 dans la note interprétative qui interdit notamment d'utiliser les numéros de compte pour dissimuler l'identification du pays où réside l'institution financière qui gère le compte.

L'ACPR considère que ces « vIBAN » sont en réalité de véritables comptes de paiement proposés en France par les autres établissements européens *via* l'entité française. Outre la vigilance qui incombe aux établissements européens susmentionnés, tout établissement français devra aussi exercer la vigilance sur les produits qu'il contribue à distribuer et tenir compte de l'ensemble des informations pour exercer sa vigilance sur ses clients.

Les établissements clients considèrent que l'utilisation de vIBAN facilite les réconciliations d'opérations de collecte des flux opérés en devise locale pour le compte de ses clients, en lieu et place de l'utilisation de références dans les motifs de virements entrants, ou encore par rapport au traitement de ces paiements à l'aide de fournisseurs de services de paiement, ou encore à partir de solutions de comptes groupés.

Une autre offre similaire a également été retirée du marché à un moment proche de celui où l'enquête a été conduite.



Cas 5a – Service impliquant des IBAN virtuels étrangers associés à un compte de paiement français

* *
*

L'ACPR analyse le cas d'usage 5a comme des comptes de paiement à part entière tenus par les établissements étrangers partenaires.

Les vIBAN étrangers sont fournis à l'établissement français et utilisés pour offrir des comptes dans d'autres devises aux clients français, mais sont en réalité des comptes de paiement à part entière offert par l'établissement étranger, qui devrait appliquer l'ensemble des obligations LCB-FT au titulaire de ce compte.

5.b - Fourniture d'un vIBAN français lié à un compte étranger

Plusieurs établissements ont ouvert des succursales en France afin d'émettre des IBAN français, ce qui a généré des confusions :

- dans certains cas, le même compte comportait plusieurs IBAN ou vIBAN avec différents codes pays, qui ont été utilisés pour acheminer les paiements vers le compte principal. **L'ACPR a clairement indiqué que cela n'était pas possible, le même compte ne pouvant pas être situé dans plusieurs pays.**
- dans d'autres cas, l'établissement a considéré que le compte IBAN français était détenu dans un autre pays. **L'ACPR a également précisé qu'en vertu de la norme ISO IBAN, le code pays doit refléter le pays où se trouve le compte, y compris le pays de la succursale si le compte est détenu dans une succursale**.

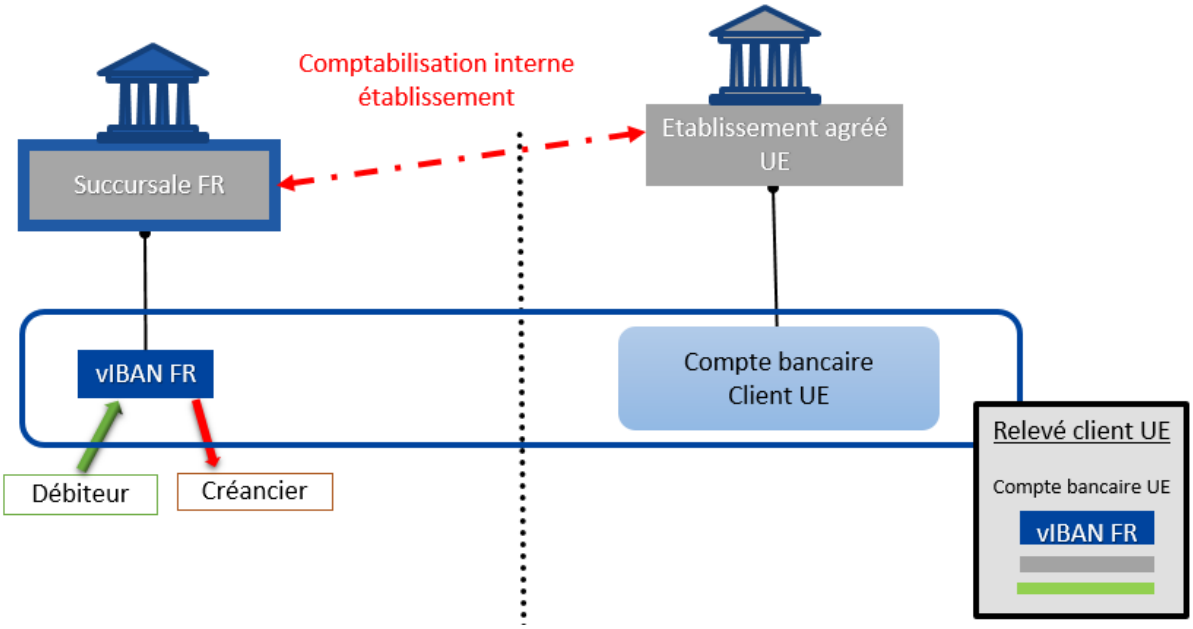
Ces principes ne font pas obstacle à l'utilisation de comptes de redirection : il s'agit notamment de comptes de paiement autonomes où un virement est automatiquement exécuté vers un compte à l'étranger à chaque fois que le compte français est crédité. Cette pratique est considérée à haut risque et nécessite une vigilance renforcée, car la redirection des flux vers une autre juridiction peut être utilisée comme moyen d'opacifier les flux financiers. Ces virements automatiques transfrontaliers sont

également utilisés par les fraudeurs dans divers types de fraude[5] afin d'éviter d'alerter la victime et compliquer les travaux des autorités répressives.

Illustration n°12 - Risques liés aux IBAN virtuels émis par une succursale pour des comptes tenus par la maison mère à l'étranger

Lorsque l'IBAN virtuel est généré par une entité d'un groupe de prestataires de services de paiement et le compte maître est tenu par une autre entité du même groupe, à l'étranger, les risques BC-FT dépendent de la qualité des échanges intragroupe : par exemple, si la succursale a un accès consolidé aux flux sur le compte tenu par l'autre entité du groupe, exerce une vigilance sur ces flux et déclare à la cellule de renseignement financier (CRF) du pays où elle est établie, les risques sont atténués.

La succursale française devrait donc avoir accès aux informations relatives aux autres comptes ou aux vIBAN détenus par le même client dans d'autres succursales ou entités du même groupe, y compris le siège social. En effet, l'analyse isolée des seules opérations passant par le vIBAN français ne permet pas de comprendre le fonctionnement global de la relation d'affaires : cela empêche par exemple de détecter que les prestations sociales versées en France sont immédiatement retirées en numéraire à l'étranger, ou que les virements entrants reçus sur l'IBAN français d'une entreprise sont immédiatement retransférés, alors même que le client ne présente aucun indice de réalité économique (absence de paiement de loyers, d'impôts, de salaires ou de cotisations sociales).



Cas 5b - IBAN virtuel FR lié à un compte de paiement étranger

Comme indiqué *supra*, certains participants justifient ce type de services pour faire échec aux pratiques de discrimination à l'IBAN. Une telle discrimination est illégale et fait l'objet de sanctions par les autorités françaises compétentes.

L'émission de services vIBAN français rattachés à un compte principal étranger est acceptée par l'ACPR sous les conditions suivantes :

[5] Par exemple, les arnaques à l'investissement où le fraudeur se fera passer pour une institution financière française ; les diverses formes d'hameçonnage ou de fraude par courriel où les fraudeurs détournent des paiements destinés à des tiers tels que les fournisseurs, les notaires.

- **Les vIBAN sont qualifiés de comptes de paiement, dont la gestion est assurée par la succursale française, laquelle a accès en temps réel à l'ensemble des opérations réalisées par le client ;**
- **Les avoirs de la clientèle sont enregistrés dans les comptes de la succursale française et peuvent être saisis en France par les autorités répressives ;**
- **La succursale applique les lois et réglementations françaises en matière de lutte contre le BC/FT et le régime de gel des avoirs, et adresse des déclarations de soupçons à la CRF française.**

L'application de ces principes est tout à fait compatible avec :

- **L'externalisation de tâches telles que la gestion informatique, la vigilance des opérations et la comptabilité dans un autre pays, de sorte que la succursale n'emploie sur le territoire français que des effectifs limités d'agents en permanence, pourvu que la succursale française dispose de ressources et compétences suffisantes et que l'ACPR ait accès à l'ensemble des informations et du personnel pour exercer sa mission de contrôle.**
- **Les comptes de redirection, où l'argent est automatiquement transféré dès réception par le compte français vers le compte étranger, et automatiquement transféré depuis le compte étranger vers le compte français lorsqu'un paiement doit être effectué à partir du compte français : ces règles automatisées peuvent avoir le même effet que les IBAN virtuels tout en garantissant le respect de la législation et de la réglementation. Ces comptes de redirection transfrontalier sont des produits à très haut risque qui nécessitent une vigilance renforcée et une vision consolidée de tous les comptes ou des vIBAN. La succursale française devrait disposer d'informations consolidées pour remplir ses obligations en matière de lutte contre le BC/FT, notamment de mener un examen renforcé et de procéder à des déclarations de soupçons auprès de la CRF française, sous le contrôle de l'ACPR.**

Ces situations sont parfois présentées par les établissements concernés comme des comptes de passage (« payable-through accounts ») qui permettent au client C d'un organisme financier A d'exécuter des opérations directement sur le compte de l'organisme financier A ouvert chez l'établissement correspondant B. La réglementation impose dans ce cas des diligences accrues fixées au 5° de l'article R. 561-21 du CMF[6]. Néanmoins, ces diligences accrues ne remplacent pas l'obligation de mener l'ensemble des diligences de connaissance de la clientèle sur le client C dans le cas d'un vIBAN attribué à chaque client renvoyant vers un compte étranger de ce client.

[6] Voir ACPR, Principes d'application sectorielle relatifs à la correspondance bancaire (https://acpr.banque-france.fr/system/files/import/acpr/media/2018/06/13/paspostcclcbft23-05pourenvoicollege.pdf)

5.c – Illustrations des risques associés à des vIBAN français lié à un compte étranger

L'utilisation d'un vIBAN pour masquer la véritable localisation des fonds contrevient à plusieurs textes européens aux enjeux importants, concernant notamment la lutte contre le blanchiment de capitaux, le financement du terrorisme et l'évasion fiscale.

1) Risque affectant l'évaluation du risque géographique

L'utilisation de vIBAN avec un code pays différent de celui du compte principal, ou d'IBAN avec un code pays erroné, génère des informations inexactes sur le pays dans lequel le compte est tenu et, par conséquent, sur l'origine ou la destination réelle des fonds. Les tiers ne peuvent pas identifier la législation nationale et l'autorité de contrôle pertinentes, ce qui fausse l'évaluation du risque géographique et empêche la mise en œuvre de mesures de vigilance complémentaires pour les opérations impliquant des pays à haut risque. Par exemple, la fraude par virement est nettement plus élevée pour les paiements destinés à certains membres de l'UE. Les réseaux criminels peuvent utiliser un IBAN local pour faciliter les escroqueries, car les victimes sont moins prudentes lorsqu'elles pensent réaliser des transferts financiers domestiques.

Illustration n° 13 – Risques liés à la neutralisation des critères de vigilance géographiques

La multiplication de virements transfrontaliers sans justification économique apparente est un critère d'analyse et d'alerte utile à la détection des sociétés écran et des lessiveuses, notamment pour l'établissement tenant le compte de la société d'où sont émis les virements. L'utilisation d'IBAN virtuels locaux peut neutraliser partiellement ce critère d'analyse : les virements transfrontaliers apparaissent comme étant des virements nationaux, du fait du code pays des IBAN destinataires. L'établissement peut toujours détecter le fonctionnement suspect du compte sur la base de l'absence de justification économique des opérations, mais il est privé du critère géographique, utile et aisément automatisable.

La neutralisation du critère géographique peut également affecter le travail des cellules de renseignement financier, notamment au moment de la priorisation et de l'affectation des cas.

2) Risques liés à la mise en œuvre de sanctions financières ciblées

Les informations trompeuses sur les pays figurant dans un IBAN entraînent également :

- **Une incertitude relative aux mesures de sanctions financières applicables :** les établissements financiers doivent identifier le pays dans lequel le compte est légalement tenu afin d'appliquer un filtrage pertinent des mesures restrictives. En effet, les listes de sanctions ne sont pas harmonisées au niveau de l'UE et des listes de sanctions nationales peuvent exister conformément à la résolution 1373 (2001) du Conseil de sécurité des Nations Unies et à la recommandation nº 6 du GAFI. L'incertitude peut donner lieu à des litiges et apparaît donc comme une source de risque juridique pour l'établissement financier teneur de compte.
- **Une incertitude sur le caractère transfrontalier ou non d'une opération et sur les obligations de filtrage des tiers** : en France, les institutions financières s'appuient sur le code pays pour

déterminer si l'opération se trouve sur le territoire français et bénéficie de la tolérance les exemptant du filtrage[7] des sanctions.

Illustration n° 14 – Risque de contournement de sanctions par l'usage d'IBAN virtuels

Le critère d'analyse géographique est important pour la détection des cas de contournement de sanctions :
- Le pays de destination des fonds peut être sous sanctions, ou connu pour héberger des personnes physiques ou morales sous sanctions.
- Le pays de destination des fonds peut être un pays connu pour ne pas appliquer les sanctions concernées (enjeu substantiel, notamment, pour les sanctions décidées au niveau national).
- L'utilisation d'IBAN virtuels FR associés à un compte principal tenu dans un autre pays pourrait donner l'illusion d'un transfert entièrement exécuté sur le territoire national, et ainsi contourner l'obligation de filtrage applicable en France[8].

Ce risque est peu matérialisé à ce stade, mais un cas a été porté à l'attention de Tracfin : l'établissement A du pays européen A fournissait au PSP B un IBAN virtuel du pays A. B avait attribué cet IBAN à une entreprise offrant des services pouvant tomber sous le coup des sanctions européennes. L'IBAN virtuel en question a été bloqué.

3) Dissimulation du pays de tenue du compte

- **L'utilisation de codes pays IBAN erronés compromet la mise en œuvre de plusieurs textes européens qui s'appuient sur le code pays de l'identifiant bancaire**

Plusieurs réglementations européennes hors du périmètre LCB-FT reposent sur le lien entre le code pays de l'IBAN et le pays de tenue des comptes, en considérant que le code pays de l'IBAN correspond au lieu de détention des fonds.

Par exemple, les règles de l'UE relatives au **recouvrement** transfrontalier des **dettes en matière** civile et commerciale utilisent le code IBAN du pays pour déterminer l'État-membre dans lequel le compte est tenu. Il en va de même pour l'article 2 du règlement (UE) 2015/848 relatif aux **procédures d'insolvabilité**[9].

Un autre mécanisme de l'UE visant à **lutter contre la fraude** à la **taxe sur la valeur ajoutée** repose sur l'IBAN des comptes de paiement impliqués dans les transferts, ou sur le code interbancaire (BIC) du PSP agissant au nom du donneur d'ordre ou du bénéficiaire, pour recueillir des informations sur les transferts transfrontaliers.

Le dispositif d'échange automatisé d'informations entre les autorités fiscales nationales peut se retrouver altéré en cas d'utilisation d'identifiants bancaires présentant un code pays différent du

[7] La France admet que les transferts nationaux - entre comptes avec un IBAN français - ne font pas l'objet d'un filtrage des sanctions par rapport aux sanctions françaises au niveau de l'opération, toutes les parties au paiement étant déjà filtrées. Cette exemption serait remise en cause si le code pays ne permettait plus d'identifier avec certitude les transferts domestiques. Les opérations entre deux comptes présentant un IBAN français pourraient alors être en réalité des transferts internationaux, sans garantie que les PSP impliqués dans le transfert filtrent leurs clients par rapport aux listes applicables en France.

[8] ACPR – lignes directrices sur le gel des avoirs https://acpr.banque-france.fr/sites/default/files/media/2021/06/23/20210616_lignes_directrices_gel_des_avoirs.pdf

[9] « (9) « les États Membres dans lesquels sont situés les actifs » signifie dans le cas : (...) (iii) les liquidités détenues sur des comptes ouverts auprès d'un établissement de crédit, l'État Membre indiqué par l'IBAN du compte ou, pour les liquidités détenues sur des comptes ouverts auprès d'un établissement de crédit qui n'émet pas d'IBAN, l'État membre dans lequel l'établissement de crédit teneur du compte à son siège ou, lorsque le compte est détenu auprès d'une succursale, d'une agence ou d'un autre établissement, l'État Membre dans lequel la succursale, l'agence ou l'autre établissement est situé. »

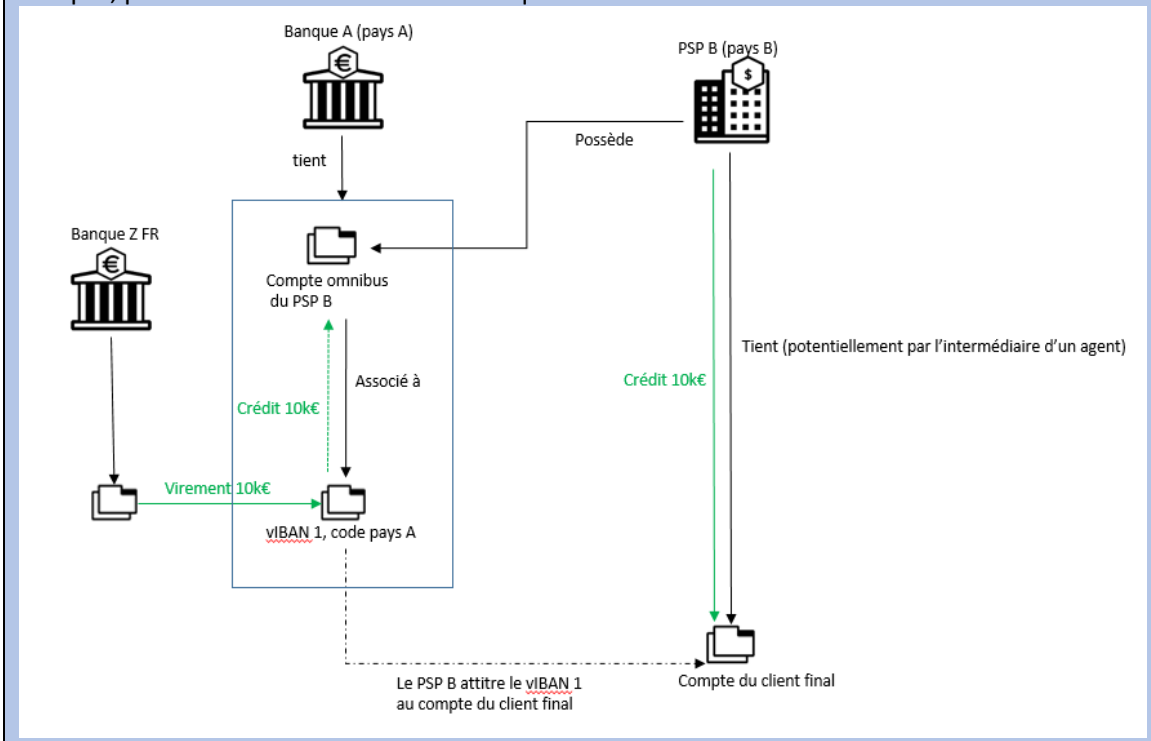
pays de tenue du compte principal : les entités financières intermédiaires doivent identifier le pays dans lequel un compte de paiement étranger est tenu, afin de se conformer à leurs obligations d'échange automatisé d'informations à des fins fiscales, en tant qu'« établissements financiers déclarants » au sens de la norme commune de déclaration de l'OCDE (Common Reporting Standard, CRS) et mis en œuvre dans l'UE par le biais des directives sur la coopération administrative.

- **L'utilisation de codes pays IBAN erronés déroute l'action des CRF et des autorités répressives**

Les procédures juridiques seront mal orientées si un compte présente l'apparence d'être tenu par un établissement donné et dans un pays donné, alors que le compte lui-même est en réalité tenu par un autre établissement ou dans un autre pays. Le risque est celui d'une mauvaise orientation des demandes des autorités compétentes : les autorités publiques doivent pouvoir identifier rapidement et de manière fiable quel établissement tient le compte et dans quel pays. L'utilisation de vIBAN présentant des codes de pays erronés induit une mauvaise orientation de leurs procédures et une perte de temps précieux qui peuvent compromettre leur action. La réactivité est un enjeu d'autant plus prégnant que les virements bancaires connaissent une accélération avec le développement des virements instantanés. Par exemple, dans le cas d'une escroquerie, la réactivité est essentielle pour récupérer les fonds.

Illustration n° 15 – Risque d'allongement des délais d'enquête en cas d'usage d'IBAN virtuels

La déconnexion entre, d'une part, l'établissement désigné par le code banque et le code pays de l'IBAN et d'autre part, l'établissement disposant d'une visibilité complète sur le client et le compte, peut occasionner des délais d'enquête.



Dans l'hypothèse où une banque du pays A génère des IBAN virtuels pour le compte omnibus de son client, un PSP du pays B, ce dernier réattribuant ces IBAN virtuels à ses propres clients (comptes tenus dans le pays B), la CRF française peut chercher à obtenir des informations sur l'utilisateur (le client final) de l'un de ces IBAN virtuels, et notamment le relevé de compte de ce client afin de suivre le cheminement de fonds. Sur la base du code banque et du code pays, elle

interroge la CRF du pays A. La CRF du pays A transmet la demande à la banque du pays A. En pratique, cette dernière ne dispose en général pas des informations demandées : seul le PSP du pays B, qui tient le compte réel du client final, peut les obtenir.

La banque du pays A peut :

- dans le meilleur des cas, obtenir les informations demandées par la CRF française en sollicitant son client, le PSP du pays B, dans le cadre de la relation contractuelle qu'elle a avec lui.
- dans le pire des cas, indiquer à la CRF du pays A qu'elle ne dispose pas des informations demandées, et que la CRF française devrait interroger la CRF du pays B, qui serait en mesure d'interroger directement le PSP du pays B.

Dans les deux cas, l'enquête subit un délai supplémentaire (potentiellement beaucoup plus important dans le second cas).

L'IBAN virtuel, dans cet exemple, pourrait fonctionnellement être comparé à un compte de passage dans le pays A, à deux nuances près :

- Le client final, au lieu de devoir entrer en relation avec deux établissements (le PSP du pays B et la banque du pays A) entre en relation uniquement avec le PSP du pays B : il s'expose à moins de mesures de vigilance.
- Là où le fonctionnement typique d'un compte de passage pourrait être détecté par la banque du pays A, l'IBAN virtuel ne permet pas une telle analyse (puisque c'est la fonction même de l'IBAN virtuel de transférer l'ensemble des fonds sur le compte réel auquel il est associé).

- **Détournement et allongement des mesures de saisies et de restrictions sur les comptes :** les forces de l'ordre françaises peuvent saisir un compte français immédiatement, sous réserve d'une confirmation ultérieure par un juge, tandis que la saisie d'un compte tenu dans un autre pays de l'UE requiert l'intervention d'un juge et plusieurs jours de mise en œuvre.

Illustration n° 16 – Risque de fraude aux finances publiques

Dans le cadre de fraudes aux dispositifs d'aides publiques limités au territoire national, le fraudeur peut utiliser un IBAN virtuel pour crédibiliser son éligibilité. Comme pour les escroqueries précitées, le compte maître est tenu dans un pays où les fonds seront très difficiles à récupérer. Cela a été constaté notamment pendant la crise COVID.

3) La dissimulation de l'origine et de la destination des flux facilite le blanchiment de capitaux

Lorsque des IBAN de codes pays multiples sont rattachés à un compte, les IBAN virtuels peuvent être utilisés à mauvais escient pour masquer l'origine, le lieu de détention ou le transfert de valeurs, qui est l'une des composantes de l'infraction de blanchiment de capitaux, au sens de l'article 3 de la directive (UE) 2018/1673 du Parlement européen et du Conseil du 23 octobre 2018[10].

Illustration n° 17 – Risque d'escroquerie

Dans le cadre d'une escroquerie, un escroc établi dans un pays tiers A, peut utiliser un IBAN virtuel avec un code pays européen, dont le compte destinataire est tenu par un PSP du pays A, pour escroquer des victimes européennes. Le client et sa banque sont mis en confiance par l'IBAN européen

[10] Site europa.eu L_2018284EN.01002201.xml

(qui peut par ailleurs crédibiliser l'histoire inventée par l'escroc) mais les fonds sont en fait versés sur un compte tenu par le PSP du pays tiers. Cela peut s'appliquer, par exemple à des escroqueries de type FOVI ou des fraudes à l'investissement. Des cas de ce type ont été traités par Tracfin.

En effet, les **établissements proposant des comptes avec des codes pays multiples sont plus exposés au blanchiment d'argent :** les rares établissements proposant différentes formes d'IBAN multi-pays représentaient environ 20 % de la valeur des demandes de retours de virement pour un motif de fraude aux moyens de paiement en France en 2022, alors que ces acteurs représentaient moins de 0,5 % des paiements reçus en France.

Illustration n° 18 – Circuit de blanchiment complexe incluant des IBAN virtuels

Tracfin a investigué un circuit de blanchiment d'escroquerie impliquant plusieurs prestataires d'IBAN virtuels français et plusieurs fournisseurs de « portefeuilles multi-devises » spécialisés dans les paiements internationaux.

1. Les fonds étaient d'abord virés sur des comptes tenus en France chez plusieurs banques en ligne, ainsi que sur des IBAN virtuels français. Les comptes associés aux IBAN virtuels étaient tenus dans différents pays européens.

2. Ensuite, les fonds étaient notamment transférés vers d'autres portefeuilles multidevises européens puis transférés à nouveau vers des comptes tenus dans des pays tiers peu coopératifs en matière de LCB-FT.

La combinaison d'IBAN virtuels permet d'opérer des transferts de capitaux complexes, et difficilement lisibles : des mouvements financiers qui apparaissent nationaux peuvent ne pas l'être, et un transfert qui semble être à destination d'un pays européen peut en réalité sortir vers un pays dont les exigences en matière de LCB-FT sont moindres. Ces mécanismes opacifient l'origine et la destination des fonds et complexifient à la fois le devoir de surveillance des établissements financiers mais aussi le travail d'enquête des autorités administratives.

4) La communication d'informations trompeuses pour les consommateurs quant au dispositif de garantie des dépôts

Le client peut croire qu'il détient plusieurs comptes auprès de plusieurs établissements (différents codes pays et codes établissement), chacun pouvant bénéficier du plafond de garantie des dépôts, alors que le PSP considère que le client ne dispose que d'un seul compte.

En outre, même si les législations européennes ont été harmonisées, la localisation du teneur des comptes a encore des conséquences en raison des différences de sa mise en œuvre qui subsistent au niveau national et parce qu'elle détermine le point de contact auprès duquel le client peut exercer son droit à garantie.

* *
*

Grille d'analyse des risques encourus par l'utilisation d'IBAN virtuels

<table>
<tr><th></th><th></th><th>Risques</th><th>Mesures d’atténuation utilisées par certains établissements</th></tr>
<tr><td rowspan="3">Cas à faible risque</td><td>CAS 1
Réconciliation des paiements</td><td rowspan="2">▪ Complexification des mesures de vigilance menées par les tiers sur les transactions financières, en raison de la fragmentation de l’activité financière du client entre plusieurs identifiants de compte (détection plus difficile de schémas « many-to-one »).
▪ Non-respect de la réglementation sur la transparence des transferts de fonds, en cas de flux sortants émis depuis un IBAN virtuel.</td><td rowspan="2">▪ Limiter l’offre de services de vIBAN aux entreprises présentant un cas d’usage clair, en excluant les cas où le vIBAN risque d’être utilisé à des fins de blanchiment.
▪ Mention de l'identifiant IEJ « Identifiant d’entité juridique » (« Legal Entity Identifier » en anglais) dans les messages de paiement.
▪ Application des obligations de déclaration des IBAN virtuels au registre des comptes bancaires.
▪ Mention dans les messages de paiement de l’IBAN virtuel et de l’IBAN du compte maître (sous réserve de pouvoir le faire d’une manière standardisée et compréhensible par les tiers)</td></tr>
<tr><td>CAS 2
Gestion analytique des flux bancaires</td></tr>
<tr><td>CAS 3
Centralisation de paiement</td><td>▪ Insuffisance des éléments de connaissance client collectés par l'établissement émetteur des vIBAN.
▪ Éventuelles infractions comptables ou fiscales en cas de mauvaise affectation des fonds dans la comptabilité de la filiale
▪ Exercice illégal de l’activité de tenue de compte par le titulaire du compte-maître des vIBAN
▪ Dissimulation du risque géographique si la centrale de paiement inclut des sociétés sises dans plusieurs pays</td><td>▪ Limiter l’offre de services de vIBAN aux groupes de sociétés dont les liens capitalistes et la réalité du groupe ont été vérifiés
▪ Vérifier que la tête de la centrale de trésorerie est autorisée à recevoir des fonds pour le compte des filiales
▪ Collecter un KYC des filiales
▪ Exercer une vigilance sur l’utilisation des IBAN virtuels et l’affectation des fonds au profit de la centrale de paiement</td></tr>
</table>

Cas à haut risque	**CAS 4** Réattribution en cascade d'IBAN virtuels	▪ Utilisation d'IBAN virtuels par des utilisateurs qui ne sont pas en relation d'affaires directe avec l'établissement émetteur des identifiants ▪ Insuffisance des éléments de connaissance client collectés par l'établissement émetteur de l'IBAN virtuel ▪ Opacification de l'identité de l'utilisateur réel du compte ▪ Complexification de la vigilance sur les opérations pour l'établissement teneur de compte et pour les établissements tiers ▪ Exercice illégal d'une activité d'encaissement de fonds pour compte de tiers ▪ Utilisation des IBAN virtuels comme de véritables comptes de paiement par des tiers ▪ Apparence pour les tiers d'un compte de paiement ouvert au nom de l'utilisateur, selon les mentions des messages de paiement et relevés	▪ Qualification de compte de paiement, déclaré au registre des comptes bancaires en tant que compte à part entière (cette déclaration est intégrée dans le paquet AML6) ▪ Interdire la distribution des vIBAN en tant que comptes de paiement et limiter l'utilisation des vIBAN à la réception de flux pour des utilisateurs effectifs faisant l'objet d'un recueil de KYC ▪ Limiter l'offre de services de vIBAN aux PSP ou agents enregistrés ▪ Limiter et assurer un suivi du nombre d'IBAN virtuels émis ▪ Limiter les contreparties admises à recevoir des flux sortants ▪ Lorsque le client est PSP, recueillir des informations générales sur les mesures de vigilance LCB-FT appliquées par le PSP client à l'égard de sa propre clientèle, et mettre en place des procédures de collaboration pour la réalisation des diligences. ▪ S'assurer que les paiements sont destinés au titulaire du compte principal lui-même (place de marché ou agent immobilier), ou que ce tiers est habilité à percevoir des paiements pour compte de tiers
	CAS 5 a et b Fourniture d'IBAN de code pays différent du compte de paiement	▪ Opacification du risque géographique pour les tiers ▪ Non-respect des sanctions financières ciblées applicables par l'établissement financier émetteur et les établissements tiers ; ▪ Mauvaise orientation des CRF et des services répressifs (demandes envoyées au mauvais pays). ▪ Compromission de plusieurs réglementations européennes, notamment le recouvrement de dettes, les procédures d'insolvabilité et le régime CESOP de lutte contre la fraude à la TVA ▪ Communication d'informations trompeuses pour les consommateurs quant au dispositif de garantie des dépôts (le client peut penser qu'il détient plusieurs comptes auprès de plusieurs établissements, chacun pouvant bénéficier du plafond, alors qu'en réalité il ne dispose que d'un seul compte)	▪ Solution alternative, utilisation de comptes réels comme comptes de redirection, sous réserve d'une justification économique établie et d'une vigilance des opérations prenant en compte le niveau de risque élevé ; ▪ En l'absence de concordance du code pays avec le pays de tenue du compte, analyser les IBAN virtuels comme des comptes de paiement. Ils sont alors considérés comme des comptes de redirection, à risque élevé. Comme tout compte désigné par un IBAN français, l'IBAN virtuel émis sous le code pays FR doit être géré sous la responsabilité de l'entité française, les avoirs des clients sont enregistrés dans les comptes de l'entité française et peuvent y être saisis ; l'entité applique les lois et réglementations françaises en matière de lutte contre le BC/FT et le régime de gel des avoirs, et adresse des déclarations de soupçons à la CRF française. ▪ Vue consolidée des comptes liés entre les différentes entités.

III - L'ANALYSE DE L'ACPR SUR LA REGLEMENTATION ET LES PRATIQUES D'ATTENUATION DES RISQUES LIES AUX IBAN VIRTUELS

1) Les évolutions réglementaires et législatives récentes

Les apports et risques présents par l'utilisation des IBAN virtuels ont été étudiés par de nombreuses autorités depuis 2023 :

- dans un rapport publié en 2023, Europol[11] a alerté sur le risque que les réseaux criminels exploitent la complexité induite par l'utilisation des IBAN virtuels pour opacifier l'origine de fonds illicites ;
- en novembre 2023, le GAFI[12] a publié un rapport soulignant le risque d'utilisation détournée des services d'IBAN virtuels, dès lors que la traçabilité des fonds est réduite par l'absence de localisation physique fixe et les fonctionnalités de redirection des flux ;
- en mai 2024, l'Autorité Bancaire Européenne a publié un rapport dédié aux IBAN virtuels[13], qui souligne les problématiques de transparence et de régulation soulevées par l'opacification de la localisation réelle des fonds et de l'identité des utilisateurs finaux en cas de recours à des IBAN virtuels. L'ACPR y a contribué grâce, notamment, à la présente étude ;
- en cohérence avec ce rapport, la Banca d'Italia a publié des recommandations[14] à l'égard des IBAN virtuels, et le superviseur allemand[15] conduit depuis début 2025 une revue thématique visant à évaluer l'usage des IBAN virtuels.

En parallèle de ces travaux, des précisions ont été apportées à l'échelle de l'UE :

- le règlement (UE) 2024/1624 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme[16], qui s'appliquera à compter du 10 juillet 2027, définit l'« IBAN virtuel » comme « un identifiant qui a pour effet de rediriger les paiements vers un compte de paiement identifié par un IBAN différent de cet identifiant» (article 2) ;
- l'article 22 dudit règlement dispose que « Les *établissements de crédit et les établissements financiers obtiennent des informations pour identifier et vérifier l'identité des personnes physiques ou morales utilisant tout IBAN virtuel qu'ils émettent, ainsi que le compte bancaire ou de paiement associé. L'établissement de crédit ou l'établissement financier gérant le compte bancaire ou de paiement vers lequel un IBAN virtuel, émis par un autre établissement de crédit ou établissement financier, redirige des paiements, veille à pouvoir obtenir de l'établissement émettant l'IBAN virtuel les informations permettant d'identifier et de vérifier*

[11] Europol (2023), European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg.

[12] Financial Action Task Force (FATF), Illicit Financial Flows from Cyber-Enabled Fraud, November 2023.

[13] European Banking Authority (EBA) (2024), Report on Virtual IBANs, EBA/Rep/2024/08, May 2024. EBA Report on virtual IBANs.

[14] https://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/Comunicazione-BdI-UIF-vIBAN.pdf

[15] Vedrenne, Gabriel. "German Regulator Targets Virtual IBANs." MoneyLaundering.com, 28 January 2025.

[16] Règlement (UE) 2024/1624 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ; https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401624

l'identité de la personne physique utilisant cet IBAN virtuel sans retard et, en tout état de cause, dans un délai de cinq jours ouvrables à compter de sa demande d'informations. »

- en outre, l'article 16 de la directive (UE) 2024/1640[17], qui doit être transposé en droit national d'ici le 10 juillet 2027, exige que les IBAN virtuels soient inscrits dans les registres des comptes bancaires, parmi lesquels « *le numéro IBAN virtuel, l'identifiant unique du compte vers lequel les paiements adressés à l'IBAN virtuel sont automatiquement réacheminés et les dates d'ouverture et de clôture du compte* ». Le texte précise en outre que « *dans le cas d'un IBAN virtuel, le titulaire du compte client visé au premier alinéa, point a), est le titulaire du compte vers lequel les paiements adressés à l'IBAN virtuel sont automatiquement réacheminés*. »

L'ACPR présente ici son analyse des vIBAN, dans le respect de l'état actuel de la réglementation européenne, mais également en cohérence avec les nouveaux textes européens décrits ci-dessus, ainsi qu'avec les exigences définies par le règlement (UE) 2023/1113 (règlement sur les transferts de fonds) et le règlement SEPA.

Par ailleurs, plusieurs pistes d'évolutions complémentaires possibles du droit ou des normes internationales en matière de vIBAN ont été identifiées :

■ Des informations utiles sur les registres de comptes bancaires

L'obligation de référencer les IBAN virtuels au registre des comptes bancaires, instituée par la 6ème directive de LCB-FT, apportera plus de transparence.

- Dans les cas où le détenteur du compte directement associé à l'IBAN virtuel est une autre institution financière (établissement de crédit, de paiement, de monnaie électronique ou statut similaire à l'étranger), les données suivantes pourraient être rendues disponibles :
  - Données sur le titulaire de compte, à savoir l'institution tenant le compte du client final. Ces données comprennent le pays où elle est établie.
  - Données KYC sur le client final (utilisateur).

La 6e directive donne aussi la possibilité aux Etats membres d'exiger que d'autres informations jugées essentielles aux CRF soient accessibles et puissent faire l'objet de recherches (article 16§6), même si celles-ci ne semblent pas bénéficier de l'interconnexion entre les registres européens (article 16 §7). À cet égard, il pourrait être utile de faire apparaître dans ces registres :

- l'identité de l'utilisateur du vIBAN, en plus de celle du titulaire du compte ; cette information devra pouvoir être collectée en application de l'article 23 §3 du règlement UE 2024/1624.
- les liens entre un IBAN virtuel et un portefeuille de crypto-actifs. Lorsqu'un PSCA dispose d'un compte auquel sont associés des IBAN virtuels, il peut en effet attitrer ces IBAN virtuels à des portefeuilles de crypto-actifs. Dans ce cas, il conviendrait de rendre disponible les données suivantes au registre des comptes bancaires et assimilés dans le cadre du référencement de l'IBAN virtuel :
  - Données sur le PSCA
  - Pays d'établissement du PSCA
  - Indication que l'IBAN virtuel est associé à un wallet
  - Identification du wallet associé

[17] Directive (UE) 2024/1640 du Parlement européen et du Conseil relative aux mécanismes à mettre en place par les États membres pour prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant la directive (UE) 2019/1937, et modifiant et abrogeant la directive (UE) 2015/849 ; https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401640

- Données sur le client final (client du PSCA, qui utilise le wallet associé à l'IBAN virtuel)

Un format spécifique pour les vIBAN

La création d'un format standardisé pour les IBAN virtuels faciliterait la détection des IBAN virtuels par les différents intervenants dans les circuits financiers (les contreparties, les établissements financiers opérant les flux, les bénéficiaires réels des flux).

Il ressort des réponses au questionnaire de l'ACPR que certains établissements ont attribué des formats spécifiques aux vIBAN, tels que l'attribution d'un code banque ou d'un code guichet. Toutefois, ces pratiques ne sont pas standardisées.

La Banca d'Italia a également observé chez certains intermédiaires la pratique d'utiliser un code guichet spécifique ou d'insérer dans les 12 derniers chiffres de l'IBAN dédié au numéro de compte, des caractères distinctifs fonctionnels pour rendre la nature virtuelle de l'IBAN immédiatement identifiable (par exemple, les lettres VA ou V au début du champ relatif au numéro de compte) et faciliter la surveillance des transactions.

Tracfin observe également qu'inclure dans le vIBAN le pays du compte de redirection (par exemple à la suite des lettre VA ou V), ainsi que le code banque de l'institution tenant ce compte, pourrait utilement compléter cette approche. Un tel format permettrait aux contreparties de prendre en compte le risque géographique. Si le code banque est inclus, ce format simplifierait aussi les enquêtes des autorités compétentes. Au lieu d'interroger le pays où le vIBAN a été émis (qui ne disposera en règle générale que d'informations parcellaires), l'autorité compétente pourrait interroger directement le pays où est tenu le compte maître et suivre le cheminement des fonds de manière plus rapide et efficace.

Les différences de structures de l'IBAN d'un pays à l'autre pourraient être un obstacle à une telle approche au niveau international. Les services de l'ACPR ont néanmoins échangé avec le comité technique en charge de la maintenance de la norme ISO sur l'éventualité d'une évolution de la norme, afin de permettre d'identifier l'IBAN virtuel voire le pays ou l'établissement de redirection.

2) Distinction entre la qualification d'IBAN virtuel et celle de compte bancaire ou de paiement

L'ACPR considère que le service d'IBAN virtuel ne peut pas être dissocié de la fourniture d'un compte bancaire ou de paiement, et seuls les PSP agréés dans l'UE (y compris par l'intermédiaire de succursales et d'agents) peuvent émettre et distribuer des vIBAN de l'UE.

Plusieurs situations doivent être distinguées :

Des IBAN virtuels admis sous la forme de comptes fusionnés (fournis par le même établissement, présentant le même code pays et utilisés par le même client)

L'ACPR avait accepté depuis plusieurs années la pratique de l' « IBAN virtuel » à condition que les IBAN examinés présentent des caractéristiques homogènes de comptes fusionnés : plusieurs comptes, chacun identifié par un IBAN, sont fusionnés au sein d'un compte maître identifié par son propre IBAN et reflétant toutes les opérations des comptes fusionnés. Cette analyse des IBAN virtuels garantit le respect de la réglementation en matière de transparence des transferts de fonds, qui exige que les

numéros de compte du donneur d'ordre et du bénéficiaire soient inclus dans les messages de paiement[18].

Pour qu'une fusion de comptes homogènes soit admise, les IBAN virtuels devraient être fournis par le même établissement, sous le même code pays, et utilisés par le même client que le compte bancaire ou de paiement d'enregistrement des transactions. **S'agissant des autres formes d'IBAN virtuels ne remplissant pas ces critères, chaque IBAN peut être analysé comme un compte de paiement à part entière tenu par l'établissement identifié par le code pays et le code banque de l'IBAN.**

Cette disposition ne s'oppose pas à la réception ou à l'initiation de paiements pour le compte de tiers par le client sur son propre compte, dans les conditions exigées par les lois et réglementations applicables (par exemple, être autorisé à recevoir des paiements pour compte de tiers en vertu de la directive (UE) 2015/2366 sur les services de paiement).

Le règlement (UE) 2024/1624 a créé la notion d'« utilisateur de vIBAN ». Celle-ci paraît devoir être distinguée de deux concepts voisins :

- le simple statut de payeur sur le compte (un débiteur se voit attribuer un vIBAN afin de payer son créancier, client de l'émetteur du vIBAN). Une différence paraît être par exemple que l'utilisateur de vIBAN serait celui à qui est destiné le paiement redirigé via le vIBAN ;
- Le « titulaire du compte », qui reçoit le paiement dans son patrimoine, mais destine les fonds à l'utilisateur du vIBAN. Il ne devrait pas y avoir de situation où des fonds appartiennent à un simple « utilisateur d'IBAN » en l'absence de tout titulaire de compte. On remarquera qu'autrement, le compte concerné ne se verrait pas appliquer l'ensemble des obligations de vigilance qui doivent être exercées à l'égard de la clientèle, notamment en ce qui concerne les bénéficiaires effectifs. La notion d'utilisateur de vIBAN est complémentaire de celle de titulaire du compte mais ne s'y substitue pas.

La notion d'utilisateur de vIBAN est proche de celle de bénéficiaire effectif des opérations, telle que définie à l'article L. 561-2-2 2° du code monétaire et financier, de sorte qu'avant même l'entrée en application du règlement (UE) 2024/1624, les établissements teneurs de compte devraient connaître les utilisateurs des vIBAN, en application de l'article L. 561-5 du code monétaire et financier : même si

[18] Le règlement (UE) 2023/1113 (informations accompagnant les transferts de fonds) précise (article 4.1) que « Le prestataire de services de paiement du donneur d'ordre veille à ce que les transferts de fonds soient accompagnés des informations suivantes sur le donneur d'ordre : (...) b) le numéro de compte de paiement du donneur d'ordre ». Cela empêche le payeur d'inclure tout autre numéro que le numéro de compte réellement utilisé.
L'article 4.2 du règlement (UE) 2023/1113 dispose également que « Le prestataire de services de paiement du donneur d'ordre veille à ce que les transferts de fonds soient accompagnés des informations suivantes sur le bénéficiaire de fonds : (...) b) le numéro de compte de paiement du bénéficiaire de fonds ».
La même règle s'applique aux transferts au sein de l'Union visés à l'article 5, si des comptes sont utilisés («lorsque tous les prestataires de services de paiement intervenant dans la chaîne de paiement sont établis dans l'Union, les transferts de fonds sont accompagnés au moins du numéro de compte de paiement à la fois du donneur d'ordre et du bénéficiaire»).
L'article 8 du règlement (UE) 2023/1113 impose au PSP du bénéficiaire de traiter le cas des transferts de fonds pour lesquels les informations complètes requises sur le donneur d'ordre et le bénéficiaire ne sont pas fournies.

cette dernière notion vise uniquement des personnes physiques, l'identification de la personne morale intermédiaire reste nécessaire[19].

■ Certaines formes d'IBAN virtuels devraient être considérées comme des comptes de paiement à part entière

Au regard des caractéristiques de certains produits présentés comme des vIBAN, l'**ACPR analyse la fourniture de vIBAN gérés par les clients finaux comme leur propre compte (cas 4) et la fourniture de vIBAN mentionnant un autre code pays (cas 5) comme une activité de fourniture de comptes de paiement**.

L'article L. 314-1 I du Code monétaire et financier (CMF), transposant l'article 4 (12) de la Directive sur les Services de Paiement révisée (dite « DSP2 »), définit un compte de paiement comme « un compte détenu au nom d'une ou de plusieurs personnes, utilisé pour l'exécution d'opérations de paiement ». Les services de paiement (SP) sont énumérés dans la partie II du même article, reproduisant l'annexe I de la DSP2. Parmi les SP recensés, le 3° vise l'exécution d'opérations de paiement associées à un compte de paiement.

Comme illustré dans les cas d'usage n°5a et 5b décrits ci-dessus, des identifiants bancaires dont le code pays diffère du pays de tenue du compte principal, devraient être qualifiés de comptes de paiement.

En cas de concordance avec le code pays du compte principal, et comme illustré dans le cas d'usage 4 précité, la qualification de vIBAN, telle que définie par le règlement (UE) 2024/1624 précité, ne saurait être retenue quand les services offerts sous l'apparence d'IBAN virtuels correspondent en réalité à des services de tenue de compte. La fourniture d'un ou plusieurs des services suivants au titulaire ou à l'utilisateur d'un vIBAN paraît permettre de repérer des indices permettant de considérer ce vIBAN comme un compte à part entière :

- La délivrance de relevé d'identité bancaire associant le vIBAN au nom d'une autre personne que le titulaire du compte dont l'identité a été vérifiée par l'établissement ;

- La délivrance d'un relevé de compte ou équivalent présentant un solde, sans qu'il s'agisse d'un simple sous-compte d'un compte à part entière tenu par le même établissement pour le même client ;

- L'initiation d'opérations de paiement depuis l'identifiant fourni vers des tiers librement choisis, le cas échéant à l'aide d'interfaces programmables (peu important quel numéro de compte d'émission apparaît dans les messages de paiement).

- L'exécution d'opérations de paiement à destination de contreparties autres que le titulaire du compte destinataire de la redirection ;

- L'exécution d'opérations de paiement entre plusieurs identifiants fournis par un établissement à un même client.

Lorsque les IBAN virtuels sont qualifiés de comptes bancaires ou de paiement à part entière au regard des critères décrits supra, les procédures exercées à leur encontre en application d'autres

[19] C'est l'interprétation des autorités italiennes : cf Banca d'italia et UIF *Indicazioni per i soggetti obbligati sull'applicazione degli obblighi in materia antiriciclaggio nell'apertura e gestione di conti di pagamento dotati di IBAN virtuali,* 12 décembre 2024. Ces autorités considèrent aussi, comme l'ACPR, qu'un simple payeur n'est pas un bénéficiaire effectif de l'opération.

réglementations (notamment en matière de saisies ou de réquisitions) doivent être similaires à celles exercées à l'égard de comptes français, sauf interprétation contraire des autorités compétentes dans leur domaine. Par conséquent, la succursale émettant les IBAN virtuels est soumise aux obligations de tout établissement proposant des comptes de paiement à l'égard des autorités compétentes. L'organisation interne de l'établissement entre son siège et ses succursales pour la gestion des comptes ne saurait justifier un allongement des délais de traitement, une limitation des données disponibles ou un allègement des procédures mises en œuvre.

Des observations complémentaires peuvent être apportées :

a. Émission d'IBAN autorisée en vertu du principe de liberté d'établissement

La fourniture d'IBAN avec un code de pays spécifique ne devrait être possible que pour les prestataires de services de paiement disposant d'un établissement (entendu comme le siège social ou une succursale) dans le pays concerné, conformément au principe de liberté d'établissement. Cela découle du fait que les registres nationaux ne peuvent techniquement attribuer un code interbancaire, qui est un élément clé des IBAN, qu'aux seuls établissements locaux.

En conséquence, un établissement souhaitant proposer un IBAN FR à sa clientèle doit ouvrir une succursale en France soumise à la réglementation financière sectorielle (DSP2, EMD2, CRD, MIFID). Cette succursale devrait être soumise aux procédures de contrôle interne de l'établissement.

b. La succursale française doit être considérée comme responsable de la tenue d'un compte de paiement en France, afin de se conformer à la norme ISO relative aux IBAN.

Conformément à la norme[20] ISO relative aux IBAN, un vIBAN, comme tout IBAN, désigne un établissement financier teneur du compte et l'État membre dans lequel le compte est effectivement détenu.

Par conséquent, **un IBAN doit nécessairement refléter la succursale dans laquelle le compte est tenu**. Ainsi, les succursales françaises qui émettent des IBAN avec un code pays FR doivent toujours être considérées juridiquement comme les teneurs de ces comptes en France. Dans la pratique, les **succursales en charge de la tenue des comptes devraient enregistrer les avoirs des clients dans leurs comptes** (y compris dans leurs déclarations fiscales).

Cela n'empêche pas la succursale de conserver les fonds auprès du siège de l'établissement (les passifs envers les clients figurant dans les livres de la succursale sont compensés par une créance à l'égard du siège social). Il est aussi possible que plusieurs tâches de la succursale soient externalisées dans d'autres lieux (par exemple, au siège), notamment la tenue de livres, la surveillance des opérations et les prestations informatiques, à condition que la succursale assure juridiquement la tenue de compte et reste responsable des activités externalisées.

Par suite, les flux financiers opérés à l'aide d'IBAN français devaient être soumis à la réglementation et à la supervision nationale en matière de LBC-FT. L'inscription des comptes dans les registres de la

[20] La norme ISO IBAN (ISO 13616-1) définit un IBAN comme une « version étendue du numéro de compte bancaire de base (BBAN), destinée à être utilisée à l'international, qui identifie de manière unique un compte individuel auprès d'un établissement financier spécifique, dans un pays particulier ».
Un numéro de compte bancaire de base BBAN est un identifiant qui identifie de manière unique un compte individuel détenu auprès d'un établissement financier spécifique dans un pays donné, et qui comprend l'identifiant bancaire de l'établissement financier qui gère ce compte.
Un identifiant bancaire est un « identifiant qui identifie de manière unique l'établissement financier et, le cas échéant, la succursale de cet établissement financier gérant un compte ».

succursale, en conformité avec la norme ISO 13616-1, ne s'oppose pas à ce que les tâches de gestion de compte soient mises en œuvre à un autre endroit.

Comme décrit précédemment, le compte de la succursale française peut fonctionner comme un compte de redirection, les fonds étant automatiquement redirigés du compte français vers un compte à l'étranger : de telles règles automatisées peuvent avoir le même effet que les IBAN virtuels tout en garantissant le respect de la réglementation. Comme évoqué ci-dessus, il s'agit d'un produit à haut risque du point de vue de la lutte contre le BC/FT et qui nécessite que la succursale française dispose, notamment dans le cadre de ses obligations déclaratives et de vigilance, d'une vision consolidée des opérations de ses clients, couvrant l'ensemble des IBAN.

c. Conditions requises pour une succursale pour obtenir un passeport en France

Au regard du mécanisme de passeport européen, l'ACPR analyse les risques liés aux IBAN virtuels de la manière suivante :

- BC/FT : les risques BC/FT mentionnés ci-dessus résultent principalement du fait qu'un vIBAN opacifie la zone géographique de situation du compte principal et qu'il peut en découler le non-respect de la réglementation applicable en matière de lutte contre le BC/FT (à savoir, celle de l'État-membre d'accueil). Pour ces raisons, l'ACPR requiert des établissements, lors de la notification d'une succursale en vue d'obtenir des IBAN français, i) de **s'assurer de la prise en compte des exigences françaises en matière de LCB-FT** (ex. pour les exigences de connaissance du client et de résidence d'un responsable LCB sur le territoire national) et ii) d'**informer les consommateurs qu'ils sont soumis à la législation française**. Les procédures de contrôle interne de l'établissement doivent permettre de prendre en compte ce risque.

- Protection des consommateurs : dans les cas où la succursale offre ses services aux consommateurs français, l'ACPR demande aux établissements, lors de la notification d'une succursale en vue d'obtenir un IBAN français, de i) veiller à ce que les **exigences françaises en matière de protection des consommateurs** (y compris le recours au médiateur français) soient prises en compte et ii) informer les consommateurs qu'ils relèvent de la législation française. Les procédures de contrôle interne de l'établissement doivent permettre de prendre en compte ce risque.

- Une identification claire des opérations impliquant une clientèle française : lors de la notification d'une succursale en vue d'obtenir des IBAN français, l'ACPR demande aux organismes d'être en mesure de **pouvoir reconstituer, à des fins de reporting, le périmètre exact des opérations traitées pour les clients utilisant des IBAN français** et de le déclarer à l'ACPR.

- Clarification technique des comptes détenus par l'établissement : afin d'avoir une vision claire des flux de paiement et d'éviter les conflits de normes, l'ACPR refuse les fonctionnalités techniques reposant sur le rattachement de plusieurs IBAN de codes pays différents à un compte maître unique.

3) La maîtrise des risques BC-FT associés aux vIBAN par les établissements financiers

Au terme d'une analyse conjointe de l'ACPR et de Tracfin, et de manière similaire à l'analyse publiée en 2024 par la Banca d'Italia[21], certaines mesures paraissent pouvoir atténuer les risques de BC-FT associés aux IBAN virtuels.

■ La mise en œuvre de procédures préalables à la distribution d'IBAN virtuels

Préalablement à la fourniture d'IBAN virtuels et conformément à l'obligation de recueillir et d'actualiser les informations relatives à l'objet et à la nature de la relation d'affaires selon des modalités renforcées en cas de produit à risque élevé (articles L. 561-5-1 et L. 561-10-1 du Code monétaire et financier), l'établissement financier doit s'assurer que l'émission d'un IBAN virtuel réponde à un besoin économique clairement identifié, et documenter l'utilisation prévue (*cf*. les différents cas d'usage présentés dans ce rapport).

Au terme d'une évaluation préalable des risques associés à la mise en service de vIBAN, et conformément à l'article L. 561-4-1 du code monétaire et financier et à l'article 2 de l'arrêté du 6 janvier 2021 relatif au dispositif et au contrôle interne en matière de LBC-FT, des mesures de gestion et d'atténuation des risques identifiés doivent être mises en place. Celles-ci peuvent inclure par exemple :

- la limitation des clients éligibles à ce service (PSP ou non-PSP, groupes de sociétés),
- la limitation des fonctionnalités offertes (nombre d'IBAN virtuels par client, conditions de création et suppression des IBAN virtuels…),
- la limitation de l'utilisation des IBAN virtuels à la réception de flux,
- ou encore la limitation des contreparties pouvant émettre ou recevoir des fonds.

Lorsque le titulaire du compte principal est un organisme financier, y compris un prestataire de services sur crypto-actifs, et que sont offerts les services de correspondance transfrontalière visés par l'article L. 561-10-3 du Code monétaire et financier, l'établissement teneur de compte doit se conformer aux obligations prévues par cet article et par l'article R. 561-21[22]. Dans les cas de services de correspondance rendus au sein de l'espace économique européen, le paragraphe 13 des principes d'applications sectorielle de l'ACPR et les paragraphes 8.18 et 8.19 des orientations de l'ABE rappellent que l'approche par les risques peut conduire à devoir appliquer certaines des diligences relatives à la correspondance transfrontalière : notamment, recueillir des informations générales sur les mesures de vigilance LBC-FT appliquées par l'organisme financier client à l'égard de sa propre clientèle, que l'organisme financier client s'engage à fournir sur demande les données relatives à ses clients et leurs opérations. L'organisme financier titulaire du compte peut également avoir un engagement contractuel à coopérer concrètement et collaborer activement avec l'établissement teneur du compte principal pour les besoins de la LBC-FT.

■ Un renforcement des procédures de vigilance des opérations

Comme mentionné par l'ACPR dans son analyse sectorielle des risques de BC/FT[23], des mesures de vigilance particulières doivent être mises en place.

---

[21] https://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/Comunicazione-BdI-UIF-vIBAN.pdf

[22] Voir Principes d'application sectorielle relatifs à la correspondance bancaire publiés par l'ACPR (https://acpr.banque-france.fr/system/files/import/acpr/medias/documents/20230629_asr_lcb_ft_2023.pdf).

[23] Analyse sectorielle des risques, juin 2023, § 2.2.1.9.

L’utilisation de vIBAN par les clients doit donc faire l’objet d’un suivi proportionné au risque associé au client et au service rendu (nombre de vIBAN associés au compte principal, possibilité de recevoir des paiements de tiers, caractéristiques et localisation des entités pour lesquelles les vIBAN sont demandés).

La vigilance des opérations réalisées à l’aide du vIBAN devrait reposer sur l’analyse du fonctionnement global du compte maître mais également, séparément, de chaque vIBAN, afin de vérifier la cohérence entre l’objectif initialement déclaré et l’utilisation effective des vIBAN. Cette vigilance doit inclure les risques associés à la réattribution des vIBAN.

Annexe 1 : Chiffres relatifs au nombre de vIBAN et au volume des opérations

- Nombre d'IBAN virtuels

Le nombre de vIBAN est généralement illimité ou n'est soumis qu'à une limite technique (1 000 000 ou 999 999).

Sur la base des chiffres déclarés, non exhaustifs, le nombre moyen de vIBAN utilisés par client est très hétérogène. Il convient de noter qu'en moyenne un seul vIBAN est attribué par personne, tandis que les entités juridiques utilisant des vIBAN ont plusieurs vIBAN liés à un seul compte de paiement : il est logiquement très élevé pour les clients des établissements financiers (plus de 40 000 vIBAN par établissement financier), beaucoup plus élevé que pour les sociétés non financières (33 vIBAN par client).

- Volume des transferts via un vIBAN

En janvier 2023, le montant des opérations réalisées par des iBAN virtuels s'est élevé à au moins 4 milliards d'euros, pour un nombre de 1,7 million de vIBAN.

Types de clients	Nombre de clients utilisant un ou plusieurs vIBAN fin 2022	Nombre total de vIBAN actifs fin 2022	Montant de la transaction en janvier 2023 à l'aide d'un vIBAN
Établissements financiers	18	731 004	664 967 608
Entreprises non financières	18 458	610 669	3 283 552 371
Personnes physiques à des fins non professionnelles	372 832	387 280	49 395 657
Autre : 1 loi sur les associations 1901	1	117	2 681 737
Total	391 309	1 729 070	4 000 597 374

- Personnes physiques, principaux utilisateurs d'IBAN virtuels

Bien que seuls 4 établissements proposent de tels services aux particuliers pour leurs besoins non professionnels, ceux-ci sont les principaux utilisateurs de services de vIBAN, en nombre (95 %, soit 372 832 sur 391 309 à fin 2022). La plupart de ces clients s'appuient principalement sur les services d'un même établissement.

Dans la grande majorité des cas déclarés, l'utilisation d'un vIBAN pour les flux de clientèle de détail permet à l'établissement d'offrir des services qu'il ne fournit pas lui-même, à savoir l'accès au réseau SEPA (355 229 vIBAN) ou, dans une moindre mesure, des identifiants bancaires étrangers (17 600 vIBAN).