La Lettre du trésorier N°443 • juin 2026

POINT DE VUE SUR LA CONFORMITÉ

TOKENISATION ET STANDARD ISO 20022 : COMMENT FAIRE CONVERGER LES LUTTES CONTRE LA FRAUDE (LCF) ET CONTRE LE BLANCHIMENT ET LE FINANCEMENT DU TERRORISME (LCB-FT)

Par Corina Fontaine, senior advisor, expert Paiements & Infrastructures de marché, Onepoint, et Alexandre Marion, avocat associé, La Tour International

Le secteur des paiements traverse une double révolution dont les effets conjugués méritent d'être examinés à l'aune des obligations de conformité. D'un côté, la *tokenisation* – accompagnée des wallets numériques, cartes virtuelles et IBANs virtuels – réduit efficacement l'exposition des données sensibles et renforce la lutte contre la fraude (LCF). De l'autre, la migration mondiale vers la norme ISO 20022, effective depuis novembre 2025 pour les institutions financières, transforme en profondeur la structure des messages de paiement : là où les formats historiques transmettaient des données minimales, ISO 20022 introduit une richesse informationnelle inédite (identifiants normalisés, informations détaillées sur les parties, références commerciales) qui ouvre de nouvelles perspectives pour la lutte contre le blanchiment et le financement du terrorisme (LCB-FT).

Ces deux évolutions sont porteuses de progrès réels. Mais elles modifient aussi la nature des risques et redistribuent les capacités d'analyse entre acteurs. C'est précisément cette sophistication croissante des usages qui invite à examiner comment les marchands assujettis à la LCB-FT, et particulièrement les plus petits d'entre eux, peuvent tirer parti de ces transformations sans en subir les angles morts.

PRINCIPE DE PROPORTIONNALITÉ

Les innovations technologiques du secteur financier – *tokenisation*, *wallets* numériques, cartes virtuelles, IBANs virtuels – constituent des avancées significatives pour la sécurité des transactions et la lutte contre la fraude. Il convient néanmoins d'examiner comment les accompagner d'une réflexion sur leur articulation avec les obligations LCB-FT auxquelles sont soumis certains marchands, afin que ces deux objectifs se renforcent mutuellement plutôt qu'ils n'entrent en tension.

Le cadre européen LCB-FT reconnaît le principe de proportionnalité : les attentes réglementaires sont modulées en fonction des capacités financières, techniques et humaines des assujettis. Pour les entreprises (PME, ETI) concernées, la transition vers la *tokenisation* soulève une question pratique nouvelle : comment maintenir une connaissance suffisante des flux financiers dans un environnement où les référentiels traditionnels évoluent ? La question est particulièrement concrète pour certaines catégories de marchands assujettis (biens de grande valeur, métaux et pierres précieuses, biens culturels) qui sont soumis à une obligation de moyens en matière de LCB-FT et à une vigilance renforcée en matière de sanctions internationales. En outre, le cadre européen sur la LCB-FT rappelle souvent que les attentes réglementaires dépendent des moyens financiers, techniques et humains de chacun. Or si les très petites entreprises (TPE) assujetties à la LCB-FT constatent trop souvent que l'affirmation de bon sens reçoit peu de traduction pratique, elles sont encore plus nombreuses à constater que l'évolution vers la *tokenisation* brouille les réflexes historiques sur la connaissance des flux financiers.

L'évolution soulève assurément un enjeu très concret pour certains marchands assujettis (ceux des biens de grande valeur, des métaux précieux et pierres précieuses, et des biens culturels), tenus à une obligation de moyens sur la LCB-FT mais à une obligation de résultat lorsqu'il s'agit de ne pas commercer directement ou indirectement avec des personnes sanctionnées.

LE CAS DES PAIEMENTS PAR CARTE

Dans le modèle de la *tokenisation* des paiements par carte, le numéro réel de la carte bancaire (le PAN pour *Primary Account Number*) est remplacé par un identifiant numérique unique, un jeton appelé *token*, généré par les réseaux de cartes ou par l'émetteur. En réduisant l'exposition des données sensibles, la *tokenisation* limite les risques de fraude liés au vol ou à la compromission des numéros de carte. Toutefois, la généralisation de ce modèle abaisse également la nature de l'information accessible aux marchands assujettis à la LCB-FT, alors qu'ils sont pourtant tenus de connaître tout de leurs clients (procédure dite de « know your customer », KYC), particulièrement lorsque la loi leur impose d'augmenter leur vigilance. La *tokenisation* tend en effet à dissocier la cohérence entre porteur, adresse de facturation et instrument de paiement – informations qui alimentent habituellement l'analyse des risques qui doit être conduite par le marchand assujetti à la LCB-FT. Dès lors, pour ces derniers, la capacité à identifier l'origine, la destination et la nature des fonds – notamment dans le contexte croissant des crypto-actifs – dépend en partie de la lisibilité des informations transmises par les acteurs de la chaîne de paiement.

C'est pourquoi une collaboration structurée entre marchands assujettis et prestataires de services de paiement (banques acquéreuses, banques émettrices, réseaux de cartes) apparaît comme une piste de convergence naturelle. Ces acteurs disposent de la capacité à déchiffrer la *tokenisation*. Une logique de partage d'informations, encadrée contractuellement et calibrée selon les profils d'assujettis, permettrait de réconcilier les impératifs de la LCF et ceux de la LCB-FT dans un modèle cohérent et opérationnel.

L'OFFRE DES ACTEURS FINANCIERS À DESTINATION D'UNE CLIENTÈLE D'ASSUJETTIS À LA LCB-FT

Le marché comprend parfaitement que la *tokenisation* présente des bénéfices évidents en matière de cybersécurité. En réduisant l'exposition des données sensibles, elle limite efficacement les risques de fraude liés à la compromission des numéros de carte. Mais elle modifie également la nature des risques. La carte ne constitue plus l'élément central de l'identification : elle devient un simple instrument d'accès à un compte et à un écosystème numérique très varié – devises, crypto-actifs, monnaie électronique, *wallets*. C'est précisément cette sophistication croissante des usages qui fragilise la capacité des marchands assujettis à exercer leurs obligations LCB-FT : là où la carte permettait d'établir une cohérence entre porteur, adresse et instrument de paiement, la *tokenisation* dissout cette lisibilité sans nécessairement la remplacer par un dispositif équivalent à destination des assujettis.

La question n'est donc pas tant celle de la *tokenisation* en elle-même que celle de l'outillage mis à disposition des marchands pour maintenir, dans ce nouvel environnement, une connaissance suffisante de leurs clients et des flux qu'ils traitent – notamment lorsque la loi leur impose de renforcer leur vigilance et de connaître l'origine ou la destination des fonds associés à une transaction.

LE LUXE COMME VECTEUR DE BLANCHIMENT : ILLUSTRATION D'UN CAS D'USAGE IMPLIQUANT LA CARTE

L'un des schémas de blanchiment aujourd'hui surveillés par les institutions financières est l'achat et la revente d'articles de luxe, souvent désigné sous le terme de *resell luxury laundering*. Le secteur du luxe présente plusieurs caractéristiques qui facilitent ce type d'opérations : une forte liquidité du marché secondaire ; des produits dont la valeur est stable ou croissante ; et un rapport valeur/volume élevé, facilitant transport et revente. Certaines références iconiques peuvent ainsi être revendues rapidement sur des marchés internationaux, parfois à un prix supérieur à leur prix d'achat.

Le mécanisme du *resell luxury laundering* consiste à transformer des fonds d'origine douteuse en actifs physiques facilement revendables, puis à récupérer des liquidités d'apparence légitime. Dans ce type de montage, la détection ne repose plus uniquement sur l'identification d'un instrument de paiement frauduleux, mais sur l'analyse d'un comportement global : achats multiples de biens de luxe ; utilisation d'instruments récents ou fragmentés ; dispersion géographique des transactions ; revente rapide via des plateformes.

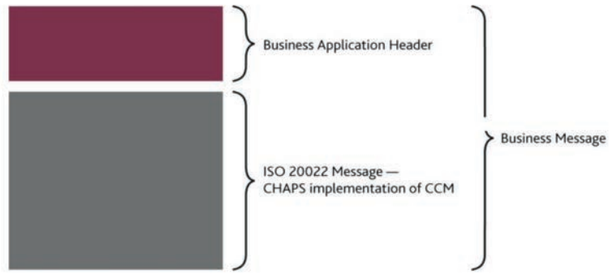
En protégeant l'instrument de paiement, la *tokenisation* impose de déplacer les capacités de détection vers une analyse plus avancée des données.

ISO 20022 : VERS UNE NOUVELLE INTELLIGENCE DES PAIEMENTS ET DE LA CONFORMITÉ

La migration mondiale vers la norme ISO 20022, effective depuis le 22 novembre 2025 pour les institutions financières, représente une évolution majeure pour l'industrie des paiements. Contrairement aux formats historiques de messagerie financière, la norme ISO 20022 permet d'intégrer des données beaucoup plus riches et structurées dans les messages de paiement. Cette évolution offre plusieurs bénéfices, tant pour la LCF que la LCB-FT. En effet, les messages ISO 20022 peuvent notamment inclure (i) des identifiants normalisés tels que le LEI (*Legal Entity Identifier*), (ii) des informations détaillées sur l'émetteur et le bénéficiaire et (iii) des références commerciales associées à la transaction.

Focus sur la norme ISO 20022

Dans le cadre de la mise en œuvre d'ISO 20022, il est possible d'introduire la norme ISO 20022 Business Application Header (BAH), conformément à la recommandation des lignes directrices HVPS+ (*High Value Payments Systems+*). Le BAH (voir ci-dessous) précède le message principal de la norme ISO 20022 et contient des informations pertinentes concernant le contenu de cette instruction de paiement.
Collectivement, le BAH et le message ISO 20022 constituent le business message d'entreprise, comme illustré dans le diagramme ci-dessous.



Une détection plus efficace des comportements frauduleux

Grâce à ces données enrichies, les banques peuvent développer des modèles analytiques plus sophistiqués permettant l'analyse comportementale des clients, la détection de schémas de fraude transfrontaliers et l'identification de réseaux criminels. Les systèmes d'intelligence artificielle peuvent ainsi exploiter un volume d'informations beaucoup plus important pour identifier les anomalies.
Les réseaux internationaux tels que Visa et Mastercard occupent également une position stratégique dans cet écosystème. En tant qu'opérateurs des infrastructures de paiement par carte, ils disposent d'une vision globale des transactions à l'échelle internationale. Cette position leur permet d'identifier des « patterns » de fraude à grande échelle, de partager des alertes avec les banques émettrices et de renforcer les modèles d'analyse antifraude.
La combinaison entre les données enrichies d'ISO 20022, les technologies de *tokenisation* et les capacités d'analyse des réseaux cartes ouvre ainsi la voie à une détection plus rapide et plus précise des comportements suspects.

A quoi sert le BAH ?

- Le BAH contient des informations clés pour le traitement d'un paiement en un seul endroit. Voici des exemples de champs au sein du BAH : « Partie de », « Partie à », « Identification de la définition du message », « Identificateur du message d'entreprise » et « signature numérique pour l'authentification/non-répudiation ».
- Le BAH peut être utilisé dans diverses situations pour faciliter le traitement et l'acheminement des instructions de paiement. Par exemple, il peut être utilisé pour informer le destinataire que les éléments textuels du message professionnel peuvent contenir des caractères non latins, ou pour informer le destinataire du service professionnel au sein duquel ce message est échangé (par exemple, SWIFT InterAct) lorsque le message métier est utilisé dans plusieurs services.
- Le BAH peut être utilisé lorsque l'expéditeur estime que le destinataire n'a pas reçu le message d'origine, lorsque l'expéditeur envoie une copie du message d'origine, un duplicata de l'original ou un duplicata d'une copie du message d'origine. En outre, il peut contenir des signatures numériques et des clés cryptographiques sécurisant le contenu du message sous-jacent. Les utilisations précises qui seront prises en compte seront dictées par les champs choisis pour remplir le message.
- Il existe un certain nombre de facteurs stratégiques pour l'utilisation du BAH (harmonisation avec les normes de messagerie HVPS+ adoptées dans d'autres juridictions qui l'ont ou le mettront en œuvre). ISO 20022 BAH peut faciliter cela en permettant aux champs requis spécifiquement à des fins de traitement dans un système individuel d'être placés dans le BAH plutôt que dans le *Customer Communications Management* (CCM).

La Lettre du trésorier N°443 • juin 2026
POINT DE VUE SUR LA CONFORMITÉ

Du point de vue du garant, la méthode de l'évaluation des pertes attendues repose sur l'étendue des pertes supportées en cas de défaut de l'emprunteur au titre du financement garanti. Cette approche suppose d'abord de calculer les pertes attendues en cas de défaut à partir de la probabilité de défaut de l'emprunteur et du taux de recouvrement de la créance attendu en cas de défaut. Ces pertes attendues au titre du financement garanti et le coût d'opportunité du capital du garant permettent ensuite d'obtenir le coût de la garantie.

Dans le contexte actuel de volatilité des taux d'intérêt et de dégradation de la qualité de crédit de certaines entreprises, seule l'application de commissions de garantie déterminées rigoureusement pour chaque garantie financière est à même de limiter efficacement l'exposition du garant ou de l'emprunteur à un risque juridique ou fiscal.

Malgré la complexité croissante des instruments de paiement, les données plus importantes permettent aux assujettis à la LCB-FT d'analyser plus finement le contexte économique d'un paiement, si la richesse informationnelle est associée aux capacités analytiques des banques et des réseaux de paiement. Pour les marchands exposés, et particulièrement les plus petits d'entre eux, l'évolution ouvre des perspectives importantes : une meilleure identification des parties impliquées dans une transaction, un enrichissement des contrôles de filtrage (sanctions, listes noires) et une compréhension plus fine du contexte économique du paiement.

LE RÔLE CENTRAL DES BANQUES DANS LA DÉTECTION DE LA FRAUDE

Dans ce contexte, les banques jouent un rôle déterminant dans la prévention et la détection de ces schémas de fraude. En tant qu'émetteurs des instruments de paiement et gestionnaires des comptes, elles disposent d'une vision privilégiée sur l'identité des titulaires via les procédures de KYC, les comportements transactionnels des clients et l'historique des paiements et des flux financiers. Les banques exploitent ces données au sein de leurs dispositifs LCF et LCB-FT afin d'identifier des signaux d'alerte tels que des achats répétés dans plusieurs boutiques de luxe, des montants élevés sur des cartes récemment émises, des transactions réalisées dans plusieurs villes en quelques heures et des paiements fractionnés pour éviter les seuils de vigilance.

Lorsqu'un comportement suspect est détecté, les banques peuvent bloquer la transaction, demander des vérifications complémentaires au client et effectuer une déclaration de soupçon auprès des autorités compétentes. Elles constituent ainsi la première ligne de défense dans la lutte contre les flux financiers illicites, mais elles ne doivent pas oublier que les données des transactions de leurs clients sont aussi surveillées par d'autres assujettis à la LCB-FT et que ces derniers ont besoin d'être alimentés en données de paiement.

UN NOUVEL ÉQUILIBRE

La transformation des paiements marque un changement de paradigme. La sécurité ne repose plus uniquement sur la protection des instruments et de leurs données sensibles, mais sur la capacité à exploiter intelligemment les données associées aux transactions. La norme ISO 20022 enrichit la compréhension des flux en apportant une granularité inédite d'information. Les banques, PSP et réseaux de cartes deviennent les pivots de cette intelligence collective, en agrégeant, analysant et redistribuant les signaux de risque.

Dans ce nouvel équilibre, la LCB-FT ne peut plus être appréhendée de manière isolée et doit devenir une véritable offre commerciale pour les marchands, à commencer par ceux assujettis à la LCB-FT et particulièrement les plus petits d'entre eux, qui n'ont pas la capacité analytique du secteur financier. C'est à raison de cette évolution que les marchands assujettis pourront efficacement œuvrer à la LCB-FT. ■