racine AVOCATS

Flash Info

Décembre 2022

Publication des Orientations de l'Autorité Bancaire Européenne (« ABE ») relatives à l'utilisation de solutions d'entrée en relation à distance conformément à l'article 13(1) de la Directive (EU) 2015/849

Les Orientations relatives à l'utilisation de solutions d'entrée en relation à distance conformément à l'article 13(1) de la Directive (EU) 2015/849 (dite « **5ème directive anti-blanchiment** ») (les « **Orientations** »), publiées par l'ABE **le 22 novembre 2022**, ont pour objet de définir des pratiques européennes communes portant sur le développement et la mise en œuvre de mesures de vigilance avec la clientèle qui sont fiables et sensibles aux risques dans un contexte d'entrée en relation à distance.

Ce document entrera en vigueur dans les six mois suivants sa publication dans toutes les langues officielles au sein de l'Union Européenne.

Vous trouverez ci-après une description des principaux apports de ce document.

I. La mise à jour des politiques et procédures internes pour insérer des éléments sur l'entrée en relation à distance

Les Orientations détaillent les éléments qui doivent être mentionnés dans les politiques et procédures des établissements assujettis concernant l'entrée en relation à distance :

- Une description générale de la solution mise en œuvre pour collecter, vérifier et enregistrer les informations pendant toute la durée de la procédure d'entrée en relation à distance. Cela inclut des explications sur **les principales caractéristiques et le fonctionnement de la solution** ;
- Les situations dans lesquelles la solution d'entrée en relation à distance peut être utilisée, en précisant les catégories de clients, les produits et les services qui sont éligibles à cette solution ;
- Les étapes qui sont entièrement automatisées et celles nécessitant l'intervention humaine ;
- Les contrôles mis en œuvre pour assurer que la première transaction avec un nouveau client est exécutée une fois que les mesures de vigilance lors de l'entrée en relation ont bien été appliquées.

II. La pré-évaluation de la solution d'entrée en relation à distance

Les Orientations prévoient en outre que les établissements assujettis doivent effectuer une pré-évaluation de la solution d'entrée en relation à distance et insérer dans leurs politiques et procédures internes les éléments suivants :

- Une évaluation de l'adéquation de la solution concernant la complétude et l'exactitude des données et documents à collecter, ainsi que la fiabilité et l'indépendance des sources d'information utilisées ;
- L'évaluation de l'impact de l'utilisation de la solution d'entrée en relation à distance sur les risques auxquels les établissements assujettis sont exposés, en ce compris les risques de blanchiment de capitaux et de financement du terrorisme, les risques opérationnels, de réputation et juridiques ;
- L'identification des mesures d'atténuation et des actions de remédiation éventuelles pour chaque risque identifié dans le cadre de l'évaluation susmentionnée ;
- Des tests pour évaluer les risques de fraude incluant les risques d'usurpation d'identité et des risques de sécurité et des autres technologies de communication et d'information ;
- Un test de bout-en-bout du fonctionnement de la solution visant les clients, les produits et les services identifiés dans les politiques et procédures interne sur l'entrée en relation à distance.

III. La vigilance constante de la solution d'entrée en relation à distance

Les Orientations précisent que la solution d'entrée en relation à distance doit être contrôlée de façon constante pour que les établissements assujettis puissent s'assurer qu'elle fonctionne conformément à leurs attentes. A cette fin, leurs politiques et procédures internes devront décrire :

- Les étapes qui seront prises pour satisfaire une qualité, une complétude, une exactitude et une adéquation continue des données collectées pendant la procédure d'entrée en relation à distance, qui doivent être proportionnées aux risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont exposés ;
- Le périmètre et la fréquence de ces revues régulières ;
- Les circonstances qui vont déclencher des revues ad hoc, notamment dans les cas suivants :
    - Changements du risque de blanchiment de capitaux et de financement du terrorisme auquel les établissements assujettis sont exposés ;
    - Les anomalies dans le fonctionnement de la solution détectées au cours d'activités de contrôles, d'audits ou de supervision ;
    - Une augmentation apparente des tentatives de fraude ;
    - Des changements du cadre légal et règlementaire.

IV. Correspondance de l'identité du client dans le cadre de la procédure de vérification

Les Orientations prévoient également que les solutions d'entrée en relation à distance mises en œuvre par les établissements assujettis doivent permettre, au minimum, dans le cadre de leur procédure de vérification que :

- Il y a une correspondance entre l'information visible de la personne physique et la documentation fournie ;

- Quand le client est une personne morale, elle est publiquement immatriculée, le cas échéant ;
- Quand le client est une personne morale, la personne physique qui la représente a le pouvoir d'agir en son nom et pour son compte.

Quand les solutions utilisées ne permettent pas aux clients d'interagir avec l'employé qui exécute la procédure de vérification, les établissements assujettis doivent :

- S'assurer que la photo ou la vidéo est prise dans des conditions de visibilité adéquates et que les propriétés requises sont capturées avec la clarté nécessaire pour permettre une vérification exacte de l'identité du client ;
- S'assurer que la photo ou la vidéo est prise au moment où le client fait l'objet de la procédure de vérification ;
- Exécuter des vérifications de détection de la vie, qui peuvent inclure des procédures où une action particulière du client est demandée pour vérifier qu'il est présent lors de la session de communication ou qui peut être utilisée sur la base de l'analyse des données reçues et qu'elle n'exige pas une action spécifique de la part du client ;
- Utiliser des algorithmes fiables et forts pour vérifier si la photo ou la vidéo prise correspond à l'image extraite du document officiel appartenant au client.

En sus de ces mesures, les établissements assujettis doivent, quand le risque de blanchiment de capitaux et de financement du terrorisme est proportionnel au risque associé avec la relation d'affaires, utiliser une ou plusieurs des mesures listées ci-dessous pour augmenter la fiabilité de la procédure de vérification :

- Le premier paiement est effectué sur un compte au nom du client dans un établissement assujetti localisé au sein de l'Espace économique européen ou d'un pays tiers soumis à des obligations de lutte contre le blanchiment de capitaux ou le financement du terrorisme qui ne sont pas moins robustes que celles imposées par la 5ème directive anti-blanchiment ;
- Envoyer un mot de passe généré de façon aléatoire au client pour confirmer sa présence durant la procédure de vérification. Le mot de passe doit être à usage unique et limité dans le temps ;
- Capturer des données biométriques pour les comparer aux données collectées au moyen d'autres sources fiables et indépendantes ;
- Contacter le client par téléphone ;
- Envoyer un email ou un courrier au client.

L'ensemble de ces éléments de nature explicative doivent permettre d'accompagner les établissements assujettis dans l'utilisation des nouvelles technologies pour la mise en œuvre de leurs obligations de vigilance lors de l'entrée en relation. En outre, les Orientations précisent que (i) dès lors que les conditions énumérées par celles-ci sont respectées par les établissements assujettis et (ii) que celles-ci sont autorisées par le droit national, le choix des solutions technologiques relève de la discrétion des établissements assujettis.

Auteurs

David Masson
Avocat Associé
dmasson@racine.eu

Sonia Oudjhani-Rogez
Avocate
soudjhanirogez@racine.eu