Rapport sur la conformité à travers le monde en 2020

Technologie, réglementation et avenir de la conformité en matière de criminalité financière

ComplyAdvantage

Table des matières

L'essentiel

Sanctions

Les États-Unis utiliseront une batterie de sanctions comme outils de « premier recours » au Moyen-Orient, en Asie de l'Est et ailleurs. L'Union européenne suivra de plus en plus l'exemple chinois et cherchera des alternatives et des solutions de contournement à l'approche américaine.

À retenir

Les professionnels de la conformité doivent se préparer à devoir gérer des divergences croissantes à propos des régimes de sanctions en 2020 et au-delà.

Blanchiment d'argent

Les techniques de blanchiment d'argent vont continuer d'évoluer rapidement. Elles recourront à des technologies nouvelles de plus en plus sophistiquée et à l'exploitation de personnes vulnérables. Le lien avec la cybercriminalité va se renforcer. L'afflux de fonds criminels sur les grands marchés immobiliers occidentaux va probablement s'étendre à un plus grand nombre de villes et de pays.

À retenir

Les professionnels de la conformité doivent être très attentifs à la fluidité des comportements criminels et réagir en conséquence. Il sera essentiel d'assurer un suivi plus agile des transactions.

Paysage réglementaire

Le cadre de la lutte contre le blanchiment d'argent (LCB) sera confronté à des changements sociaux et technologiques profonds, notamment le développement du cannabis thérapeutique et l'augmentation des actifs virtuels (AV). Pour ce qui est des actifs virtuels, l'UE adoptera une approche lente mais cohérente, la stratégie de la région Asie-Pacifique sera à la fois souple et diverse tandis que la politique des États-Unis sera ambitieuse sur le plan rhétorique mais fragmentée dans la pratique.

À retenir

Les professionnels de la conformité doivent rester attentifs aux changements réglementaires rapides, en particulier concernant les actifs virtuels, ainsi qu'au défi permanent que représentent les différentes réponses nationales et régionales. Les entreprises auront besoin de soutien de conseillers qui maîtrisent l'innovation et les diverses régions géographiques.

Innovation

Les établissements financiers collaboreront de plus en plus étroitement avec les autorités règlementaires pour exploiter tout le potentiel des nouvelles technologies au service de la réglementation financière (RegTech), en particulier l'apprentissage automatique. L'année 2020 devrait être une année d'intensification de l'engagement, où le « partenariat » sera un concept fort, plus particulièrement entre les secteurs public et privé.

À retenir

2020 sera probablement une période très positive pour l'engagement réglementaire, en particulier dans l'environnement fiable des « bacs à sable réglementaires » Si vous êtes dans la FinTech, impliquez-vous.

Tendances du marché

Les coûts liés à la conformité resteront probablement élevés pour les plus gros établissements financiers car la mise en œuvre des changements structurels et technologiques ne peut se faire que progressivement. Généralement plus agiles et toujours plus expérimentées, les FinTech devraient tirer quelques avantages de la situation, à la fois en tant que concurrents et partenaires du secteur institutionnel.

À retenir

Les FinTechs devront bien réfléchir à la manière dont elles se positionnent par rapport aux établissements financiers plus importants et bien implantés sur le marché ainsi qu'aux implications pour leur approche de la conformité. Une bonne conformité est importante dans tous les cas, que ce soit en tant que partenaires ou concurrents

Introduction

Bienvenue au tour d'horizon que vous propose ComplyAdvantage pour 2020, année qui marquera le trentième anniversaire de la publication par le Groupe d'Action Financière (GAFI) de son premier ensemble de 40 recommandations qui est au cœur du cadre mondial de la lutte contre la criminalité financière.

Même si cela mérite d'être célébré, de nombreux éléments de la lutte contre la criminalité financière à l'échelle mondiale sont mis à rude épreuve et en proie aux déclarations contradictoires des politiques nationales, aux inégalités économiques mondiales et aux changements socio-économiques rapides. Certaines de ces forces sont centripètes, en particulier la politique, tandis que d'autres, notamment les progrès rapides de la technologie, commencent à obliger les gouvernements et les autorités réglementaires à réfléchir, chacun à leur propre rythme certes, à un mode de réaction cohérent.

2020 devrait être une année de progrès plutôt limités dans la lutte contre la criminalité financière au niveau mondial et avec quelques revers possibles en cours de route. Les politiques internationales contradictoires des États-Unis et de leurs alliés renforcent le risque de divergence au niveau des régimes de sanctions tandis que les gouvernements restent confrontés à de multiples menaces de blanchiment d'argent, notamment l'afflux de fonds d'origine criminelle vers les marchés de l'immobilier et le lien croissant entre cybercriminalité et criminalité financière.

Les cadres réglementaires nationaux et internationaux sont en train de se fragiliser sous le poids de ces pressions, avec en particulier les défis que posent les actifs virtuels. Mais il y a des signes encourageants. Les autorités réglementaires s'engagent véritablement sur la voie de l'innovation pour renforcer la conformité et les résultats tandis que les partenariats public-privé sont également susceptibles de se développer. Il en sera de même pour la collaboration entre entreprises privées sur le marché des services financiers à mesure que les établissements institutionnels et les fournisseurs de technologies financières (FinTechs) trouveront des moyens de collaborer pour lutter contre la criminalité financière.

L'année 2020 sera probablement une nouvelle année pleine de défis. Mais nous comptons aussi sur quelques développements prometteurs.

Sanctions

Satisfaire aux exigences des différents régimes de sanctions est l'un des grands défis que doivent relever les établissements financiers opérant dans un écosystème financier international incroyablement diversifié, complexe et fluide. Le principal régime de sanctions qui préoccupe la plupart d'entre eux est celui des États-Unis, mis en œuvre et supervisé par le Bureau de contrôle des avoirs étrangers (OFAC) qui dépend du Département du Trésor des États-Unis. D'autres pays comme le Royaume-Uni et l'Australie ont leurs propres listes de sanctions, tout comme certaines organisations internationales telles que l'Organisation des Nations Unies (ONU) et l'Union européenne (UE). Les organisations et pays occidentaux ont eu tendance à axer leurs sanctions sur les mêmes cibles, en particulier contre des menaces communes liées à la prolifération des armes et du terrorisme international, mais certains signes indiquent que ces régimes de sanctions pourraient diverger de plus en plus.

Les points chauds géopolitiques

La situation la plus instable reste celle de l'Iran, pays soumis aux sanctions de l'ONU et de l'Occident essentiellement (mais pas exclusivement) en raison de ses programmes d'armement nucléaire et de missiles balistiques. En 2015, l'Iran a négocié avec les États-Unis, la Chine, la Russie, le Royaume-Uni, l'Allemagne, la France et l'UE un plan d'action global conjoint (JCPOA) pour assouplir les sanctions prises contre le pétrole, les transports maritimes et le secteur bancaire iranien en échange de limitations du programme nucléaire iranien. Cependant, en mai 2018, les États-Unis se sont retirés de l'accord et, en novembre 2018, ont réimposé des sanctions en rapport avec le nucléaire iranien. Malgré le fidèle soutien des autres signataires du JCPOA, la réimposition de sanctions américaines a gravement nui à l'économie iranienne, où le rationnement de l'essence a déclenché une vague de protestations dans tout le pays en novembre 2019. Les tensions militaires ont également augmenté dans le golfe Persique au cours de l'été en raison d'un certain nombre de provocations iraniennes, notamment l'abattage d'un drone américain et la mise en quarantaine d'un pétrolier britannique. Les tensions restent également vives avec la Corée du Nord. Le sommet de Hanoï qui s'est tenu en février 2019 entre le président américain Donald J. Trump et le président nord-coréen Kim Jong-un n'a pas abouti à la dénucléarisation de la Corée du Nord et malgré la reprise des pourparlers « au niveau opérationnel » le 05 octobre dernier, peu de progrès concrets semblent avoir été réalisés. Cela pourrait changer en 2020 avec l'éventuel « joker » du Président Trump permettant de conduire à des pourparlers en face à face pour créer une avancée lors de son année de réélection. Toutefois, au vu des discussions menées jusqu'ici, une telle avancée semble peu probable.

Un outil de premier recours

Depuis le 11 septembre, les États-Unis utilisent de plus en plus les sanctions comme principal outil pour assurer la sécurité nationale. Cependant, avec le président Trump, elles sont devenues un outil de « premier recours » car l'administration, largement soutenue, encouragée et parfois dirigée par le Congrès, a montré une préférence marquée pour les formes de coercition économique plutôt que militaire. En réponse aux actions iraniennes menées dans le Golfe persique, par exemple, les États-Unis ont choisi de sanctionner des membres du gouvernement iranien en juin plutôt que de recourir à la force militaire. Outre la crise iranienne, les États-Unis ont également étendu ou décrété des sanctions contre :

- Le régime de Nicolas Maduro au **Venezuela ;**
- Les **entreprises chinoises** liées à des violations présumées des droits humains dans la province chinoise du Xinjiang ;
- Les **fonctionnaires chinois** et de **Hong Kong** jugés responsables de violations des droits humains lors des troubles actuels à Hong Kong ; et
- Les **entités et individus russes** impliqués dans des attaques contre l'Ukraine, dans une attaque via un agent neurotoxique contre un ancien espion à Salisbury au Royaume-Uni, dans des tentatives de contournement des sanctions contre le Venezuela et dans l'ingérence dans les élections de mi-mandat de 2018, entre autres actions.

Parmi les autres champs d'actions possibles en 2020 figureront les sanctions américaines contre la Turquie pour son achat d'équipement militaire russe et contre les entreprises, individus et projets russes liés à une possible ingérence dans les élections présidentielles américaines de novembre 2020. Les États-Unis vont probablement aussi étendre leur éventail de sanctions au domaine des actifs virtuels. En novembre 2018, l'OFAC a sanctionné deux portefeuilles numériques de Bitcoin liés à des allégations de contournement des sanctions iraniennes. Et même si 2019 a été une année relativement calme à cet égard, l'utilisation croissante d'actifs virtuels par les Iraniens, les Vénézuéliens et les Nord-Coréens sera probablement un motif pour continuer de les pénaliser en 2020. En effet, l'importance croissante des actifs virtuels pour la Corée du Nord a été mise en évidence en décembre 2019 lorsque les autorités américaines ont arrêté l'expert en cryptomonnaies Virgil Griffith accusé d'avoir conseillé le régime de Pyongyang sur la manière d'utiliser des actifs virtuels pour contourner les sanctions. Le régime nord-coréen planifierait également le développement de sa propre cryptomonnaie soutenue par le gouvernement.

Les États-Unis divergent-ils du reste du monde ?

Même si l'Union européenne et d'autres États occidentaux n'ont pas toujours emprunté exactement la même voie que les États-Unis, leurs régimes de sanctions respectifs ont été suffisamment proches pour avoir un « air de famille ». Néanmoins, il y a toujours eu quelques variantes dans l'approche. Contrairement à d'autres régimes, les États-Unis recourent aussi largement à des sanctions secondaires extraterritoriales si bien que les tiers non-américains qui traitent avec les entités visées sont également soumises à des mesures exécutoires. Ceci a longtemps été un point de friction avec d'autres pays en ce qui concerne l'Iran, pays auprès duquel tant de nations ont toujours acheté du pétrole. Jusqu'à récemment, les États-Unis ont réussi à s'en accommoder en adoptant une approche pragmatique vis-à-vis des solutions de contournement que d'autres pays amis ou puissants ont mises en place pour contrer les sanctions secondaires, notamment le système de paiement financier parallèle que la Chine a instauré avec l'Iran sous l'administration Obama. Mais la sévérité croissante des États-Unis rend les arrangements plus difficiles et toujours plus légitime la volonté de mettre au point un système financier mondial alternatif non basé sur le dollar et autonome, très probablement supervisé par la Chine. Cela ne se produira pas en 2020, mais si les tensions économiques et politiques entre les États-Unis et la Chine se poursuivent, il est de plus en plus probable que cela finira par se produire, surtout si le président Trump est réélu.

L'attitude de l'UE sera déterminante pour savoir si cela se fera plus tôt ou plus tard. La réaction de l'UE face au retrait des États-Unis du JCPOA pourrait être le signe avant-coureur d'une approche plus différente. Même s'ils restent centrés sur le commerce humanitaire qui n'est pas affecté par les sanctions américaines, l'UE et les gouvernements français, allemands et britanniques ont cherché à mettre en place des moyens qui rappellent l'approche chinoise destinée à contourner les États-Unis. Tout au long de 2019, des acteurs européens ont développé une structure spécialisée baptisée « The Instrument to Support Trade Exchanges » (INSTEX) pour réaliser des échanges commerciaux avec l'Iran en dehors du dollar américain. La Chine a également manifesté de l'intérêt pour cette initiative qui, si elle couronnée de succès, donnera aux Européens et à d'autres pays les moyens de défier la politique américaine. Ce qui ne manquera d'ailleurs pas de mettre à son tour l'unité du système financier international à rude épreuve si les désaccords politiques persistent.

Quelles conséquences pour mon entreprise ?

- Les professionnels de la conformité devront surveiller de près l'imposition de nouvelles sanctions américaines en rapport avec les principaux points chauds géopolitiques que sont l'Iran, la Corée du Nord, le Venezuela, la Chine, la Russie et la Turquie en 2020. Les professionnels du secteur des actifs virtuels devront être particulièrement attentifs aux sanctions potentielles.
- Les entreprises non-américaines devront accorder une attention particulière à l'impact des sanctions secondaires, en particulier contre l'Iran, et aux réponses des autres grands acteurs mondiaux, dont l'UE, qui risquent de diverger.acteurs mondiaux, dont l'UE, qui risquent de diverger.
- Compte tenu de l'évolution rapide des régimes de sanctions, il sera de plus en plus important de disposer d'une solution souple et automatisée pour opérer un filtrage en temps réel.
- Les divergences toujours plus profondes en matière de réglementation rendront indispensable l'utilisation d'une solution de filtrage des sanctions capable de superviser non seulement les principales listes de sanctions, mais aussi toutes les listes nationales et internationales.

Blanchiment d'argent

Le blanchiment d'argent, à savoir le « nettoyage » de fonds d'origine criminelle visant à les faire paraître légitimes, est une activité florissante. En effet, l'Office des Nations Unies contre la drogue et le crime (ONUDC) estime que le montant des fonds blanchis à travers le monde en un an représente de 2 à 5 % du PIB mondial, soit entre 800 milliards et 2000 milliards de dollars américains. Le GAFI fait remarquer qu'il existe trois principaux canaux pour blanchir des capitaux : la contrebande transfrontalière, la facturation fictive de biens et de services au niveau du commerce international (connue sous le nom de blanchiment de capitaux lié aux activités commerciales ou TBMxL et le système financier.

$800Bn – $2Tn

Le montant estimé de l'argent blanchi dans le monde en un an se situe entre 2 et 5 % du PIB mondial – 2 000 milliards de dollars US..

Bien que la contrebande existe toujours, il est extrêmement risqué de la pratiquer à grande échelle si bien que les criminels font preuve d'une ingéniosité croissante au niveau des techniques utilisées pour profiter de la complexité du commerce et des finances. Et tout naturellement, le blanchiment TBML s'est développé en même temps que la mondialisation croissante de ces trois dernières décennies. Dans une étude publiée en janvier 2019, le groupe de défense et de recherche Global Financial Integrity (GFI) implanté aux États-Unis a constaté un lien étroit entre la montée en puissance du blanchiment de capitaux lié aux activités commerciales et l'augmentation des échanges commerciaux entre les économies avancées et émergentes situées en Afrique subsaharienne, au Moyen-Orient, dans la région Asie-Pacifique, plus particulièrement en Asie du Sud-Est, ainsi qu'en Amérique latine. Si bien que le risque de blanchiment TBML continuera de se développer en même temps que les échanges commerciaux. En outre, le système financier international, qui s'accompagne d'une diversité croissante de produits, de marchés, de fournisseurs et de technologies de livraison, offre aux blanchisseurs un éventail des solutions de plus en plus attractif pour créer des chaînes complexes de transactions internationales, et également virtuelles.

Schtroumpf coucou et passeurs d'argent

Le blanchiment continue de prendre des tournures uniques. Ainsi, le « Schtroumpf coucou » (ou blanchiment 2.0) a été révélé dans les médias australiens en 2019 suite à une affaire portée devant la Haute Cour concernant la responsabilité légale de parties dont les comptes ont été utilisés de manière abusive. Alors que le « schtroumpfage » de base concerne le dépôt d'espèces en plusieurs fois pour éviter toute détection suite à des opérations trop importantes, la variante du « coucou » met en scène une transaction entendue entre des parties innocentes pour masquer le transfert de valeurs entre criminels. Prenons l'exemple de parents d'un étudiant qui vivent dans un pays A et qui souhaitent envoyer de l'argent, disons 10 000 dollars, à leur enfant qui étudie dans un pays B. En parallèle, un groupe criminel opérant dans le pays B souhaite verser le même montant à un autre groupe criminel sévissant dans le pays A. Des membres d'une société de transfert de fonds feront le nécessaire pour que les 10 000 dollars des parents soient versés à leur insu sur un compte contrôlé par le groupe criminel du pays A si bien que les fonds ne quitteront jamais le pays. Entre-temps, les fonds du groupe criminel du pays B seront versés sur le compte de l'étudiant. Les employés réaliseront toutes les formalités et opérations nécessaires au sein du système afin que la transaction entre les parents et l'étudiant semble réelle et que le transfert de valeur des fonds criminels soit également bien effectué.

L'autre technique classique qui consiste à recourir à des « passeurs d'argent » est également en train d'évoluer. Un passeur est un individu recruté par des criminels, volontairement ou non, pour agir comme mandataire pour déposer des fonds criminels dans le système. Au cours des trois dernières années, les autorités en Amérique du Nord, aux États-Unis, dans l'Union européenne et dans la région Asie-Pacifique ont cherché à attirer l'attention des médias et du public sur ce phénomène. Ainsi, aux États-Unis, le FBI a lancé une grande campagne en mars 2019 contre 600 passeurs soupçonnés d'être impliqués dans un trafic d'argent et a procédé à des arrestations et des saisies en septembre 2019.

Les forces de l'ordre ont constaté l'importance de la vulnérabilité des personnes utilisées comme passeurs d'argent par des gangs criminels. Aux États-Unis, le FBI s'est montré particulièrement préoccupé par le recours croissant à des personnes âgées à faible revenu tandis qu'au Royaume-Uni et en Europe, c'est l'augmentation du nombre de passeurs d'argent chez les jeunes et les jeunes adultes qui continue d'inquiéter. Selon un rapport de septembre 2019 publié par le CIFAS, le service britannique de prévention de la fraude, le nombre de cas de passeurs d'argent impliquant des jeunes de 14 à 18 ans a augmenté de 73 % en deux ans. L'une des autres tendances qui caractérisent les passeurs d'argent est le lien croissant avec la cybercriminalité et Internet. En 2016, des recherches menées par l'Office européen de police (Europol) ont montré que 90 % des transactions identifiées dans le cadre d'une importante enquête sur les passeurs d'argent étaient liées aux produits de la cybercriminalité, notamment un large éventail de fraudes liées au commerce électronique.

En parallèle, l'omniprésence de la technologie mobile et des médias sociaux offre de nouvelles possibilités de recrutement de passeurs parmi les jeunes, soit directement, soit par le biais de l' « ingénierie sociale », une technique qui consiste à tromper une personne pour qu'elle divulgue des informations ou agisse généralement par le biais de la technologie. Aux États-Unis par exemple, le FBI a récemment souligné le rôle important que les sites de rencontre en ligne jouent désormais dans le recrutement de passeurs victimes de manipulation émotionnelle.

le cadre d'échanges crypto à crypto et pour tout établissement financier impliqué dans l'encaissement de cryptomonnaie pour la transformer en monnaie fiduciaire.

À moins d'élaborer une réglementation permettant de faire évoluer le concept de protection de la vie privée vers la notion de transparence, toute entreprise traitant de tels actifs, ou avec des entreprises qui le font, pourra être vulnérable à des fonds potentiellement intraçables.

Virtuellement en couches

Bien que la grande majorité des placements et des empilements soient encore effectués en monnaies fiduciaires (dollar américain, euro, etc.), les actifs virtuels (surtout les cryptomonnaies) sont en train de devenir une composante croissante du processus complexe d'empilement des fonds. Les cryptomonnaies « classiques » telles que le Bitcoin suscitant de plus en plus l'attention des régulateurs, 2020 sera probablement l'année d'un intérêt toujours plus important des criminels pour les cryptomonnaies confidentielles ou « anonymes », notamment le Monero, qui garantissent un plus grand anonymat à ses utilisateurs.

L'an dernier, les cas mettant en scène des cryptomonnaies confidentielles sont devenus monnaie courante. Les produits d'une cyberfraude ou d'un chantage peuvent être initialement collectés en Bitcoin puis échangés via différentes plateformes d'échange de cryptomonnaies (ou cryptobourses) contre tout un éventail d'autres cryptomonnaies, notamment des pièces de monnaie confidentielles, puis encaissés. L'utilisation de ces techniques garantit des « trous noirs » efficaces au niveau du processus d'empilement qu'il est impossible de suivre, ce qui pose des risques spécifiques pour la connaissance de ses clients (KYC) dans

En effet, les craintes du marché sont telles qu'avant même l'apparition d'une réglementation, les principales bourses de cryptomonnaie telles qu'OKExKorea, BitBay et Coinbase ont commencé à prendre des mesures préventives en retirant des cotations plusieurs cryptomonnaies confidentielles.

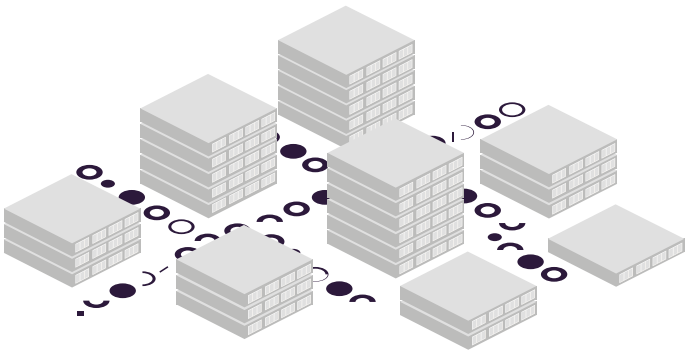
Autre domaine à surveiller, celui des places de marché en ligne pair à pair (P2P) où des particuliers donnent accès à des actifs inutilisés contre un paiement. La vulnérabilité de ce domaine a été soulignée suite à des affaires de blanchiment d'argent impliquant l'utilisation abusive de la plateforme de location de biens immobiliers AirBnB et du service d'autopartage/VTC Uber. Dans les deux cas, les « fournisseurs » d'actifs se sont entendus avec des criminels qui proposaient des locations et des déplacements en voiture factices et sur lesquels ils prenaient une commission. Une récente étude sur les jeux en ligne menée par le Royal United Services Institute (RUSI) et publiée en octobre 2019 a également mis en évidence le risque de blanchiment lié à la sphère des jeux. En effet, les joueurs en ligne peuvent souvent échanger des articles « dans le jeu » qui peuvent ensuite être reconvertis en monnaie fiduciaire dans le monde non virtuel.

En sécurité comme à la maison

En termes d' « intégration », le marché de l'immobilier devrait rester un enjeu majeur en 2020. Le problème de l'afflux de fonds criminels sur les marchés immobiliers des grandes villes occidentales a été une préoccupation concrète et croissante des professionnels de la conformité au cours de la dernière décennie, des structures sociales opaques ayant été utilisées par des bénéficiaires effectifs finaux (UBO) anonymes pour acheter des biens immobiliers d'envergure. De grandes villes américaines de même que Sydney, Hong Kong, Vancouver et Londres sont considérées comme des cibles criminelles. Ainsi, en mars 2019, le gouvernement provincial de la Colombie-Britannique a publié un rapport d'experts estimant qu'en 2018 5,3 milliards réalisés lors de transactions immobilières dans cette province avaient été financés par les produits de la criminalité, y compris par la corruption internationale.

À mesure que les gouvernements concernés adopteront des mesures pour s'attaquer à ce problème, notamment avec des ordonnances relatives au patrimoine inexpliqué (UWO) comme c'est déjà le cas en Australie et au Royaume-Uni depuis janvier 2019, il y aura probablement un effet de « déplacement » des fonds vers le marché immobilier de villes plus petites et dans d'autres pays. Le Parlement européen a récemment rapporté des cas en République tchèque, en France, en Finlande, en Grèce, au Portugal, aux Pays-Bas et en Allemagne. En plein essor, le marché immobilier allemand est particulièrement surveillé depuis que Transparency International (TI) a publié un rapport en décembre 2018 estimant que 30 milliards d'euros de fonds non identifiés étaient entrés sur le marché immobilier allemand en 2017. En novembre 2019, le parlement allemand a approuvé une nouvelle loi renforçant les règles de la lutte contre le blanchiment d'argent pour le secteur immobilier, mais sa mise en œuvre devrait prendre un certain temps.

L'incertitude politique devrait aussi entraîner un effet de déplacement similaire vers des fonds ayant auparavant afflué depuis la Chine vers le marché immobilier de Hong Kong. Avec la poursuite des manifestations contre les autorités locales, le risque d'une intervention directe de la Chine reste bien réel en 2020 si bien qu'au cours des deux derniers trimestres 2019, des agents immobiliers singapouriens et australiens ont signalé un intérêt accru de la part d'acquéreurs chinois potentiels. Il est probable que des criminels profitent de cette « poussée » du marché pour réaliser leurs propres investissements immobiliers.



Quelles conséquences pour mon entreprise ?

- Les techniques de blanchiment évoluant rapidement, les systèmes statiques de supervision des transactions sont donc toujours plus vulnérables. Les professionnels de la conformité doivent comprendre tout le potentiel que recèlent les plateformes plus innovantes pour pister les criminels.
- La nouveauté de vos produits et la vulnérabilité de votre clientèle sont deux éléments clés à prendre en compte lors de l'évaluation des risques de criminalité financière. L'exposition à des méthodes de paiement novatrices, en particulier les actifs virtuels, et des clients situés aux deux extrêmes des tranches d'âge méritent une attention toute particulière. Intégrer ces facteurs de risque à votre stratégie de conformité est crucial.
- Les entreprises opérant sur le marché de l'immobilier doivent aussi évaluer avec soin les risques et affiner les contrôles. Si les grandes villes finissent par être saturées de fonds d'origine criminelle, il est probable qu'il y aura un effet de déplacement croissant vers d'autres régions ainsi que vers des établissements financiers plus vulnérables, en particulier dans l'espace de la FinTech.

Perspectives et divergences réglementaires

Outre les risques sous-jacents de criminalité financière, les établissements financiers devront réfléchir à l'évolution des stratégies de conformité au niveau mondial, régional et national. Les tendances sociales et technologiques rendent nécessaire l'adoption d'une approche cohérente dans ce domaine, mais cette dernière est souvent entravée par des idiosyncrasies nationales à des degrés divers.

Vue par région

Loi SAFE sur le cannabis

Aux États-Unis, l'utilisation et la possession de cannabis sont illégales en vertu de la législation fédérale des États-Unis depuis l'adoption de la loi sur les substances contrôlées (CSA) en 1970. Au niveau fédéral, le cannabis est considéré comme un stupéfiant inscrit à l'annexe 1 en raison de la dépendance et des abus qu'il peut créer. Toutefois, au niveau des États, on observe une tendance croissante à la légalisation de l'usage thérapeutique du cannabis depuis les années 1990. A l'heure actuelle, 33 États américains, ainsi que le District de Columbia, Guam, Porto Rico et les îles Vierges américaines, ont approuvé des programmes d'utilisation du cannabis à des fins thérapeutiques, tandis que 11 États ont également légalisé son usage à des fins récréatives.

La tension croissante entre le point de vue fédéral- et celui des États a récemment conduit à des tentatives législatives de type « quadrature du cercle ». En avril 2019, un groupe bipartisan a présenté un projet de loi visant à garantir que les entreprises présentes sur le marché du cannabis légal puissent avoir accès au système financier légitime. En septembre 2019, la Chambre des représentants des États-Unis a adopté ce projet de loi à visée bancaire baptisé Secure And Fair Enforcement (SAFE) Banking Act et qui est maintenant examiné par le Sénat. Si une loi est adoptée, elle devra encore obtenir le consentement du président Trump.

La promulgation de la loi SAFE aurait des implications majeures pour les établissements financiers qui cherchent à augmenter leur présence sur le marché légal du cannabis. Actuellement, la loi permet aux autorités réglementaires fédérales de prendre directement des mesures pour empêcher les établissements financiers de traiter avec les producteurs de cannabis, y compris en retirant l'assurance des dépôts à l'établissement financier. Comme la Loi SAFE supprimerait ces pouvoirs, cela garantirait une sphère de sécurité aux établissements financiers et une opportunité de croissance sensible pour les entreprises produisant du cannabis légal. Pourtant, le cannabis resterait une drogue inscrite à l'annexe 1 au niveau fédéral et les entreprises opérant sur le marché du cannabis légal resteraient probablement à haut risque pendant un certain temps en raison de l'illégalité antérieure de ce commerce. Néanmoins, que la loi SAFE soit adoptée ou non, de nouveaux entrepreneurs se lanceront dans cette activité à mesure que la réglementation des États évoluera. Les établissements financiers devront donc être particulièrement vigilants à l'égard des entités ayant déjà été condamnées ou ayant des liens avec des stupéfiants illégaux.

Quelles conséquences pour mon entreprise ?

- Les professionnels de la conformité doivent aborder le marché des drogues légales en évaluant pleinement les risques de criminalité financière. Faites preuve d'une diligence raisonnable et d'un filtrage adapté lors de l'intégration de ce type de client. Veillez à ce que le filtrage et la supervision des transactions soient bien adaptés aux risques spécifiques et ménagez de la souplesse afin de pouvoir vous adapter à vos besoins évolutifs en matière de risques.

Directives AMLD 5, 6... et autres à venir

2018 et 2019 ont été des années très actives et riches en rebondissements au niveau des efforts faits par l'UE en matière de lutte contre le blanchiment d'argent. Malgré la multiplication des scandales touchant les banques d'Europe du Nord et dont les médias se sont faits l'écho, l'UE a adopté une approche « au fil de l'eau » en matière d'évolution de la réglementation. Depuis 1991, la stratégie de l'UE pour lutter contre le blanchiment s'est concentrée sur la transposition d'une succession de directives anti-blanchiment (AMLD) dans la législation nationale des États membres. En 2018, les directives anti-blanchiment (AMLD) 5 et 6 ont été publiées au Journal officiel de l'UE et tout au long de 2019, les autorités nationales ont cherché à s'assurer que leurs propres lois et réglementations étaient conformes aux nouvelles directives européennes. Les gouvernements doivent transposer la 5ème Directive LCB (5AMLD) dans leur législation nationale avant le 10 janvier 2020 et ils devront faire de même pour la 6ème Directive anti-blanchiment avant le 03 décembre 2020. De ces deux dates, c'est la Directive 5AMLD qui a l'impact le plus direct sur les établissements financiers. Alors que la Directive 6AMLD vise à créer une cohérence législative concernant les infractions en matière de blanchiment d'argent dans l'UE, la 5ème Directive étend les réglementations LCB aux cryptomonnaies et aux échanges de cryptomonnaies via les plateformes d'échange de cryptomonnaies et améliore l'accès aux données sur la propriété des entreprises et sur les personnes politiquement exposées (PPE). Une plus grande clarté réglementaire sera plus particulièrement bénéfique aux actifs virtuels, un important sous-secteur de la FinTech, tandis qu'une meilleure information des clients aidera toutes les entreprises dont les équipes de conformité sont limitées (voir l'encadré ci-dessous pour plus de détails).

La 5ème Directive anti-blanchiment (5AMLD) en bref :

- **Cryptomonnaies :** elle fournit une définition juridique de la « cryptomonnaie » et fait de ceux qui négocient ces devises des « entités obligées » en vertu de la règlementation sur la lutte contre le blanchiment et le financement du terrorisme. Les cryptobourses et les fournisseurs de portefeuilles doivent désormais s'inscrire auprès de leur organisme de réglementation national.
- **Cartes prépayées :** le montant pouvant être stocké ou utilisé mensuellement sur des cartes prépayées sans contrôle préalable supplémentaire sera ramené de 250 à 150 euros tandis que le plafond des transactions en ligne sera lui abaissé à 50 euros.will be reduced to €50.
- **Propriété effective :** les registres nationaux des entreprises bénéficiaires effectives finales (UBO) deviendront publics d'ici au 10 janvier 2020 et seront interconnectés par une plateforme centrale européenne d'ici le 20 mars 2021.
- **Personnes politiquement exposées (PPE) :** les gouvernements doivent dresser et publier une liste des PPE « fonctionnelles », à savoir celles occupant des fonctions publiques importantes, tant au niveau national qu'au sein d'organisations internationales.
- **Pays tiers à haut risque :** les entités obligées ayant des relations avec des clients implantés dans des pays tiers présentant des risques élevés devront faire preuve d'une diligence raisonnable accrue et assurer la surveillance continue et renforcée de la relation client.
- **Biens de grande valeur :** les personnes faisant le commerce de biens de grande valeur, notamment d'œuvres d'art ou d'antiquités, de pétrole, d'armes, de minerais et de métaux précieux ou encore de tabac, sont maintenant des entités obligées.

La 6ème Directive anti-blanchiment (6AMLD) en résumé :

- **Infractions :** une infraction désormais unique pour le blanchiment d'argent et 22 infractions sous-jacentes, dont la cybercriminalité et la criminalité environnementale.
- **Responsabilité :** étend la responsabilité pénale aux personnes morales, notamment les entreprises et leurs partenaires.
- **Sanctions :** requiert une peine d'emprisonnement maximale d'au moins quatre ans pour une infraction pour blanchiment d'argent, soit une augmentation d'un an.

Les prochaines étapes vers une éventuelle 7ème Directive anti-blanchiment concerneront probablement une tentative de combler les lacunes des réglementations actuelles pour tous les actifs virtuels (et pas seulement les cryptomonnaies ; voir notre discussion sur les cryptomonnaies stables ci-dessous) ainsi que l'extension de la réglementation à un plus large éventail de technologies financières. Néanmoins, à la lumière des scandales bancaires en cours, une révision de l'approche stratégique plus large de l'UE en matière de lutte contre le blanchiment, plutôt que le « maintien du statu quo », sera certainement une priorité majeure pour 2020. Lors de leur réunion de décembre 2019, les ministres des finances de l'UE ont demandé à la Commission européenne de formuler des recommandations visant à améliorer la coopération transfrontalière en matière de lutte contre le blanchiment d'argent, y compris la création d'une nouvelle agence européenne de lutte contre le blanchiment. Les ministres ont également demandé une analyse pour déterminer si les directives AMLD pouvaient être transformées en règlements de l'UE, ce qui les rendrait directement applicables et exécutoires par l'UE. Si l'on s'en tient aux piètres résultats obtenus jusqu'à maintenant, il est peu probable que l'UE prenne rapidement des décisions sur ces questions. Cependant, il existe des signes encourageants comme quoi l'UE commence à comprendre la nécessité d'une réponse plus proactive à la criminalité financière.

Quelles conséquences pour mon entreprise ?

- Si vous êtes exposés à des actifs virtuels dans l'UE, la 5 Directive AMLD est une bonne nouvelle pour vous. Plus de clarté dans le secteur de la cryptographie devrait renforcer la confiance et réduire les risques. Cependant, attention au fait que l'UE pourrait ne pas traiter tous les actifs virtuels de la même manière (voir la rubrique « Actifs virtuels » ci-dessous).
- Tous les établissements financiers, et plus particulièrement les plus petites entreprises et les FinTechs, devraient chercher à tirer parti du renforcement de la transparence des entreprises européennes afin d'améliorer la connaissance KYC et de réduire les risques. Échangez avec un fournisseur de services de filtrage innovant pour savoir comment procéder au mieux.

Fusion asiatique

L'Asie–Pacifique a suivi la tendance de l'Europe visant à renforcer la coopération économique et politique régionale, mais lentement. En 2008, l'Association des nations de l'Asie du Sud–Est (ANASE) s'est transformée en un organisme de type européen tandis qu'en 2015, les États d'Asie du Nord et d'Asie centrale se sont réunis au sein de l'Union économique eurasienne (EAEU) dirigée par la Russie. Fondé en 2018 pour encourager les investissements de toute l'Eurasie dans la région, le Centre financier international d'Astana (AIFC) au Kazakhstan est une plaque tournante essentielle de ce regroupement. De nombreux pays asiatiques participent également à l'initiative chinoise Belt and Road Initiative (BRI), ou Nouvelle route de la soie, un projet commercial et infrastructurel multinational associant des liaisons terrestres et maritimes à travers toute l'Asie. Ces efforts débouchent aussi sur des engagements destinés à collaborer contre la criminalité financière, tant dans un cadre organisationnel qu'au niveau bilatéral, à l'instar de l'initiative entre les banques centrales indonésienne et philippine annoncée en septembre 2019 afin de renforcer l'alignement de la réglementation LCB.

Mais, au–delà des grands mots, la diversité réglementaire de la région reste très importante. En effet, à travers toute la région Asie–Pacifique, 35 juridictions différentes, dont les grands centres financiers mondiaux de Tokyo, Hong Kong, Singapour, Shanghai et Mumbai, possèdent encore leurs propres cadres nationaux de lutte contre le blanchiment. Qui plus est, les gouvernements nationaux continuent d'aborder la réglementation LCB avec des degrés de sophistication et un rythme variable, notamment vis–à–vis de l'appétit régional croissant pour le FinTech. Contrairement aux pays occidentaux, une partie non négligeable de la population de cette région n'avait jusqu'à maintenant aucune relation avec les banques et dépendait des flux de trésorerie au quotidien et des économies qu'elle pouvait faire. Avec l'essor des économies nationales et du commerce en Asie du Sud, du Sud–Est et de l'Est et l'omniprésence de la communication mobile, les plateformes numériques sont devenues la réponse naturelle face au besoin rapide de la région d'un type d'infrastructure financière plus formel, en particulier pour les paiements sécurisés. Il n'est donc pas surprenant que plusieurs des FinTechs les plus importantes et à la croissance la plus rapide au monde soient des plateformes de paiement telles qu'Alipay en Chine, Paytm en Inde ou Gojek en Indonésie.

Plusieurs des principales économies régionales ont été pionnières dans la définition de stratégies novatrices face aux défis LCB que pose cette révolution FinTech. Ainsi, la loi Payment Service Act (PSA) de Singapour de 2019 a assoupli le cadre réglementaire des systèmes de paiement pour les banques et toutes sortes de FinTech en pleine évolution, tout en prévoyant des exemptions en matière de LCB basée sur le risque pour les entreprises à faible risque, notamment les fournisseurs de services monétaires nationaux. Cependant, la diversité des réponses réglementaires face à l'innovation du secteur reste grande, même de la part des nations pionnières en la matière. À Singapour, la banque centrale du pays, l'autorité monétaire de Singapour (MAS), a supervisé le développement de son approche en matière d'actifs virtuels. En revanche, le nouveau régime d'actifs virtuels de la Malaisie lancé en janvier 2019 est géré par l'organisme Securities Commission Malaysia (SC), plutôt que par la banque centrale Bank Negara Malaysia qui a procédé en février 2018 aux premières modifications pertinentes de la règlementation LCB vis–à–vis des actifs virtuels.

Même si elles sont rapides, les réponses nationales idiosyncrasiques risquent de poser plus de difficultés à moyen terme pour parvenir à un alignement réglementaire régional, tout comme pour l'attribution des rôles et des responsabilités à des institutions non homologues qui ont une expertise ou des perspectives différentes vis–à–vis du secteur comme nous le verrons plus loin. Cela risque d'avoir des conséquences commerciales négatives pour les entreprises de la FinTech ayant des ambitions transfrontalières et mettra en lumière les différences nationales ainsi que les vulnérabilités potentielles face à la criminalité financière. Une réponse souple face à l'innovation est bien entendu bienvenue, mais comme d'autres régions en ont fait l'expérience, si les réglementations ne sont pas universelles dans la pratique, il est alors plus facile pour les criminels financiers de s'arranger entre eux.

En effet, l'exhaustivité et l'efficacité des régimes de lutte contre le blanchiment en place restent très diverses à travers la région. De nombreux pays ont eu du mal à satisfaire aux normes les plus élémentaires du GAFI. L'Indonésie s'efforce de faire adopter rapidement les lois et règlements dont elle a besoin pour achever sa transformation, passant de son inscription sur la liste noire du GAFI en 2012 au statut d'observateur et de membre aspirant aujourd'hui. Mais même les membres de longue date du GAFI sont confrontés à des problèmes. Le Japon, par exemple, a fait l'objet d'évaluations sévères lors de trois précédentes séries d'évaluations mutuelles réalisées par le GAFI, ce qui a conduit l'Autorité japonaise des services financiers (FSA) à exhorter son secteur financier à « jouer davantage le jeu » dans l'optique de la quatrième série d'évaluations mutuelles lancée au dernier trimestre 2019. Pendant ce temps, l'Australie, pourtant décrite par le GAFI en 2015 comme ayant un « régime mature », est impliquée dans un scandale bancaire majeur depuis novembre, depuis qu'une des quatre grandes banques du pays, Westpac, a été pointée du doigt pour ses défaillances importantes en matière de LCB. De plus, une enquête menée par le GAFI concernant les secteurs non financiers impliqués dans le marché immobilier australien (agents immobiliers, avocats et comptables) a été interrompue en novembre 2019. S'investir dans le développement de normes n'implique pas toujours de les respecter semble–t–il et les difficultés que rencontrent le Japon et l'Australie révèlent que les entreprises opérant dans des économies très développées ne devraient pas s'accommoder de risques même faibles en matière de LCB.

Quelles conséquences pour mon entreprise ?

- Les marchés de l'Asie–Pacifique représentent une opportunité majeure pour les FinTechs. Peu de pays sont aussi friands de technologies que ceux de la région Asie du Sud–Est. Des approches réglementaires nationales progressives encourageront encore cette tendance.
- Cependant, les professionnels de la conformité, en particulier pour des activités transfrontalières, doivent surveiller de près les divergences réglementaires concernant les FinTechs, même parmi les pays les plus en pointe dans le domaine. Au–delà de la rhétorique politique, un alignement régional semblable à celui de l'UE est loin d'être atteint.
- Les professionnels de la conformité doivent également rester conscients que les économies développées de la région ne sont pas nécessairement « à faible risque », comme le rappelle le scandale Westpac. Les entreprises exposées à des secteurs plus risqués dans quelque juridiction que ce soit devraient rester vigilantes.

Actifs virtuels

Les actifs virtuels ont déjà été mentionnés à plusieurs reprises dans ce dossier et nous considérons le développement de cadres réglementaires pour ce sujet en apparence exotique comme un défi majeur et constant pour 2020. Ces deux dernières années, il y a eu une volonté politique, émanant du plus haut niveau et toujours plus forte, d'envisager une approche plus uniforme en la matière. En octobre 2018, le GAFI a explicitement déclaré que tous les actifs virtuels étaient soumis à ses recommandations en matière de LCB/FT. Cependant, comme nous l'avons précisé dans la section « Fusion asiatique », les régulateurs nationaux ont eu du mal à suivre le rythme des évolutions technologiques et à maintenir un « front commun » au niveau de leurs réponses.

L'Union européenne a été un leader mondial dans ce domaine en introduisant la 5ème Directive LCB (5AMLD), mais même les progrès européens restent relativement lents. Tout au long de l'année 2019, l'Autorité bancaire européenne (ABE), l'Autorité européenne des marchés financiers (AEMF) et la Commission européenne ont entretenu des échanges permanents et qui font toujours l'objet de discussion sur la question de savoir si les actifs virtuels impliquent ou non une approche réglementaire sur mesure.

Aux États-Unis, en octobre 2019, les dirigeants de plusieurs agences fédérales, dont la SEC (Securities and Exchange Commission), ont publié une déclaration commune qui enjoint les entreprises du secteur des actifs virtuels de se conformer à la réglementation appropriée. Ces agences ont apporté davantage de précisions quant à celle à laquelle s'adresser en fonction de la question réglementaire à aborder. Néanmoins, les actifs virtuels restent toujours de la compétence réglementaire de différents organismes fédéraux selon que les actifs virtuels sont considérés comme une monnaie ou un jeton, un titre ou une marchandise. Et tout comme pour le cannabis, chaque État américain a aussi son propre point de vue sur ces actifs virtuels. Certains, comme New York, la Californie, l'Arizona et le Wyoming, cherchent à mettre en place des cadres souples pour encourager leur développement tandis que d'autres, comme le Massachusetts, n'ont pas du tout pris position.

Comme on pouvait s'y attendre, dans la région Asie-Pacifique, les approches varient du tout au tout. La Chine est favorable à l'utilisation de la blockchain comme fonction de réserve centrale mais a interdit les levées de fonds participatives (ICO) de tout actif virtuel ou cryptomonnaie qu'elle ne contrôle pas. À Singapour, l'autorité MAS qui a une vision à long terme et très ambitieuse de transactions sans friction entre actifs virtuels et monnaies fiduciaires encourage activement les banques à travailler avec les start-ups spécialisées dans les cryptomonnaies.

L'une des difficultés auxquelles sont actuellement confrontés les fournisseurs de services d'actifs virtuels, ainsi que les autorités de réglementation, est l'absence frappante de langage, de compréhension et d'approche en commun. D'un côté, le secteur des actifs virtuels évolue rapidement, sans véritable respect des définitions conventionnelles des actifs, tandis que de l'autre, les gouvernements et les régulateurs avancent à un rythme plus lent et plus régulier et tentent de faire entrer les actifs virtuels dans un cadre cognitif familier. Un bon exemple de cela est l'intérêt croissant de plusieurs pays, dont la Chine et la Thaïlande, pour le développement des cryptomonnaies stables. L'unique argument en faveur des cryptomonnaies stables est que, contrairement aux cryptomonnaies classiques, elles offrent une stabilité relative des prix. Cette stabilité s'obtient soit en garantissant la monnaie contre une marchandise non virtuelle comme l'or ou une autre cryptomonnaie détenue en réserve, soit en utilisant des algorithmes pour prendre des décisions relatives à la « masse monétaire » pour assurer le niveau de stabilité souhaité.

La réglementation des cryptomonnaies stables est cependant confrontée à un problème fondamental, à savoir que ces monnaies virtuelles ne correspondent pas toutes nécessairement aux classifications actuelles des cryptomonnaies. Ainsi, aux États-Unis, si la cryptomonnaie stable est liée à une monnaie fiduciaire, l'achat de cette cryptomonnaie pourra être considéré comme un dépôt, ce qui obligera les fournisseurs à respecter la réglementation bancaire fédérale et de chaque État. Toutefois, une réponse réglementaire aussi complète pourrait ne pas être nécessaire si les cryptomonnaies stables sont soutenues par un

algorithme. Dans certaines juridictions, le lien avec un actif sous-jacent pourrait également permettre de considérer certaines cryptomonnaies stables comme un « dérivé », c'est-à-dire un titre dont la valeur dépend des fluctuations du prix d'un actif sous-jacent. Dans d'autres cas, les cryptomonnaies stables telles que TrueUSD, qui ne détiennent pas la garde de l'actif sous-jacent, n'auront probablement pas à respecter la règlementation sur la conservation des devises, contrairement à celles concernées par cette mesure. Le lien potentiel avec les monnaies fiduciaires posera aussi des problèmes sur des bourses telles que celles de Hong Kong et du Japon où les actifs virtuels ne sont pas considérés comme des monnaies mais comme des marchandises ou des valeurs mobilières. Ce distinguo implique que, dans certains endroits, les cryptomonnaies stables pourraient ne pas être du tout définies comme des actifs virtuels en vertu des lois actuelles.

En parallèle, les organismes chargés de la réglementation prennent parfois l'industrie de vitesse s'ils ne maîtrisent pas suffisamment ce qu'il est possible de faire. Un exemple concret est la décision du GAFI en juin 2019 d'inclure une « règle de voyage » pour les transactions en actifs virtuels et qui impose aux établissements financiers de transmettre les informations du compte du donneur d'ordre et du bénéficiaire à l'établissement bénéficiaire. Le GAFI a donné aux pays jusqu'en juin 2020 pour se conformer à cette règle, malgré l'absence actuelle d'un réseau ou d'un mécanisme parapluie ayant le même rôle que le système de messagerie SWIFT pour les transactions internationales en monnaie fiduciaire. Même si des contournements techniques tels que des « oracles » ou des « chaînes latérales » peuvent servir à connecter des blockchains publiques et privées, le niveau d'interopérabilité qu'implique cette « règle de voyage » des actifs virtuels mettra du temps à se développer. La solution la plus pragmatique à court terme sera probablement de développer des normes de reporting communes par types de monnaie spécifiques ou des consortiums régionaux de bourses d'échanges et de portefeuilles. Cela pourrait ne pas satisfaire aux exigences immédiates des régulateurs internationaux, mais ce serait néanmoins une étape importante dans le processus de maturation du secteur des actifs virtuels.

Quelles conséquences pour mon entreprise ?

- Si vous êtes un fournisseur de services d'actifs virtuels ou si vous évaluez le marché, le renforcement de l'intérêt du régulateur est une évolution dans le bon sens. La clarté réduit l'incertitude.
- Néanmoins, la diversité des approches adoptées par les différents gouvernements et autorités de règlementation devrait octroyer une pause aux professionnels de la conformité, surtout si leur entreprise compte opérer au-delà des frontières intérieures des États-Unis ou des frontières internationales de la région Asie-Pacifique. Concernant les actifs virtuels, différents pays sont à des stades de développement différents, certains pays parmi les plus avancés adoptant même des approches différentes.
- En cas de doute, prenez contact avec une société de conseil qui connait bien ces marchés et assurez-vous que votre entreprise est protégée à la hauteur de son appétit pour le risque

Innovation et points sensibles

Concernant les établissements financiers, l'un des principaux stimuli de l'innovation réglementaire a été la participation accrue de la FinTech et de la RegTech au secteur, certains entrepreneurs à l'affût de nouvelles technologies ayant remis en question le caractère flou d'un cadre LCB vieux de trente ans. Les grandes banques ont également joué un rôle, en particulier celles qui ont dû faire face à des mesures réglementaires importantes à la suite de manquements. Pour bon nombre de ces grands établissements, innover leur permet de survivre.

L'apprentissage automatique

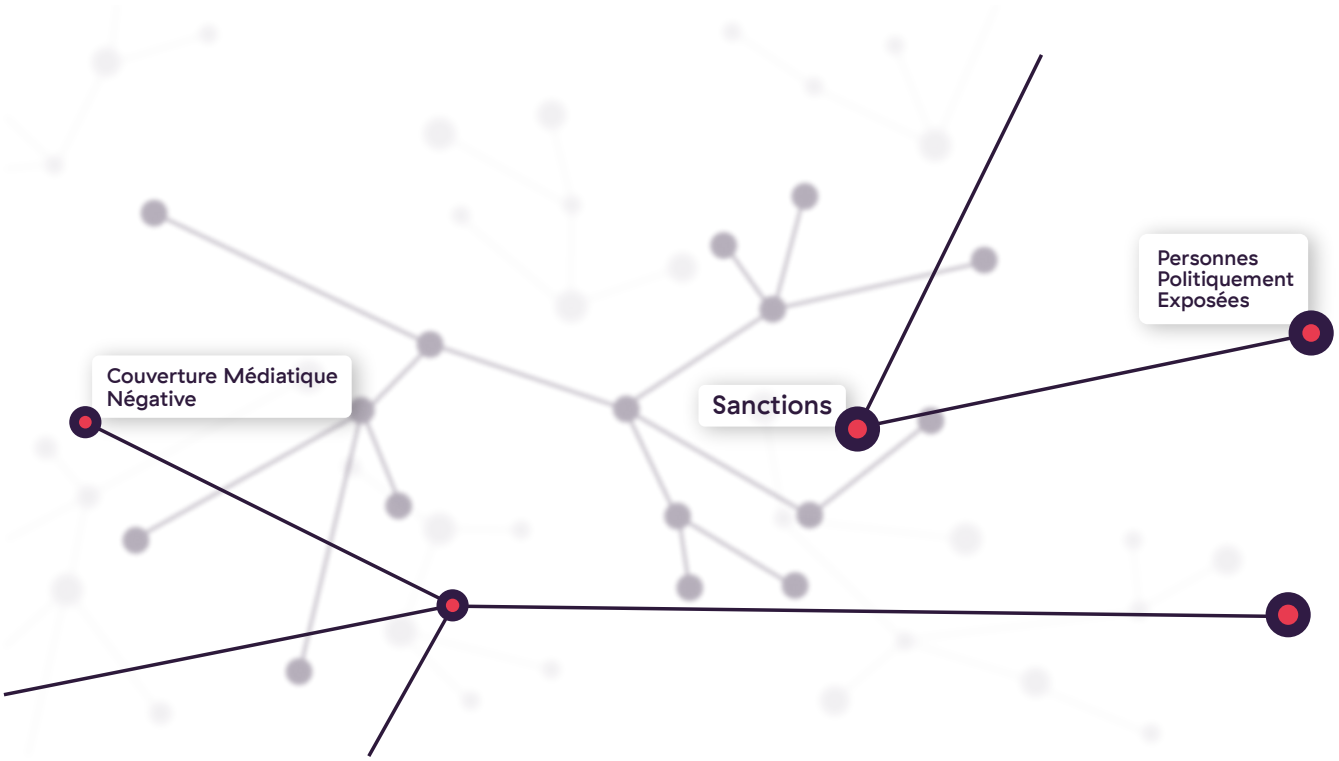
Nombreuses sont les technologies qui jouent un rôle dans l'innovation, même si l'apprentissage automatique, une forme d'intelligence artificielle (IA) s'appuyant sur des algorithmes modifiables pour identifier des caractéristiques jusqu'à maintenant non identifiées au sein de données en volume, s'avère l'une des plus prometteuses. Le développement de ce domaine a permis d'améliorer la collecte des données sur les clients grâce au traitement du langage naturel (TLN). En la matière, les algorithmes d'apprentissage ont permis de traduire plus facilement et plus rapidement la communication humaine en données lisibles par la machine. Grâce à l'utilisation du langage de programmation Python et aux bibliothèques d'apprentissage automatique, les établissements financiers peuvent intégrer de nombreux ensembles de données et normaliser les registres de clients et le comportement des clients comme jamais auparavant, ce qu'on appelle aussi la « résolution d'entités ».). Enfin, des algorithmes modifiables ont été appliqués à ces nouveaux ensembles de données intégrés pour favoriser une meilleure compréhension, améliorer sensiblement la vitesse de reconnaissance des caractéristiques, mieux identifier les comportements anormaux et réduire également le taux de faux positifs (et de faux négatifs).

Associées, ces technologies ont un impact positif et important sur les obligations de vigilance à l'égard de la clientèle (CDD), la connaissance des clients (KYC) et la supervision des transactions. En raison des risques concurrentiels qu'induisent ces initiatives, de nombreux établissements financiers hésitent à parler de l'efficacité de ces plateformes.

Toutefois, les données du marché concernant leur adoption semblent claires et positives. Ainsi, d'après une enquête réalisée auprès de 59 établissements financiers par l'Institut de la finance internationale (IIF) en 2018, 35 % d'entre eux étaient en train de tester ces technologies, 34 % utilisaient activement des techniques d'apprentissage automatique tandis que les autres prévoyaient de le faire dans un avenir proche.

Cependant, l'introduction de plateformes innovantes n'est pas toujours chose facile. Pour les banques traditionnelles qui disposent souvent de nombreuses sources de données autonomes plus anciennes, nettoyer et intégrer des données pour puiser dans une « corne d'abondance » unique peut s'avérer une entreprise coûteuse. Pour les établissements internationaux, les lois nationales sur les données qui restent hétérogènes peuvent également être une source de tensions. Il y a bien des avantages, mais ils sont plus lents à se concrétiser.

En revanche, l'introduction de nouvelles technologies s'avère plus simple pour les établissements financiers de plus petite taille et plus jeunes. En règle générale, les FinTechs trouvent plus facile de travailler en étroite collaboration avec les RegTechs pour mettre au point de nouvelles technologies, en partie parce qu'elles partagent une vision plus souple. Les collaborations FinTech–RegTech sont également efficaces pour valider des modèles et expliquer et répéter les avantages du système auprès des organismes chargés de la réglementation. Avec des régulateurs toujours plus en faveur de l'innovation, les FinTechs sont tout particulièrement bien placées pour savoir ce qui fonctionne au niveau des nombreuses technologies RegTech testées dans des environnements de bac à sable.

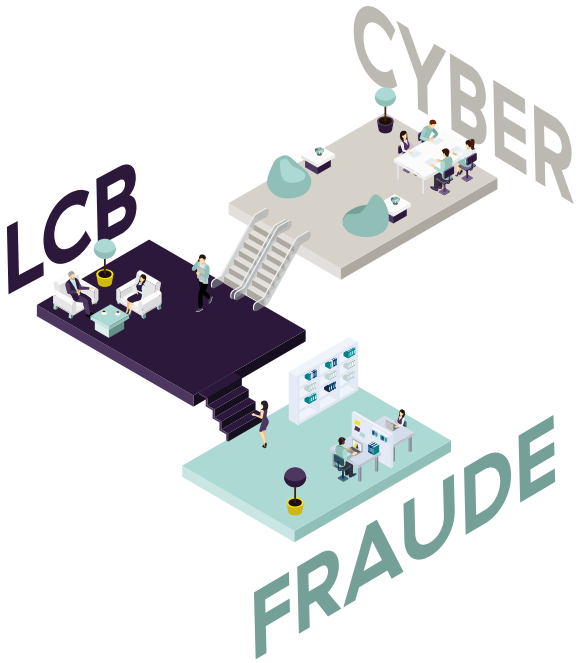


Identité numérique (IDN)

Autre nouveau concept pertinent pour prévenir la criminalité financière, l'identité numérique (IDN) qui relie directement les renseignements personnels d'une personne numérique à une « vraie » personne. L'objectif de la technologie IDN est de créer un moyen fiable d'associer numériquement des renseignements personnels. Cela permet d'identifier de manière cohérente les interactions d'un individu avec des entreprises, des administrations et d'autres personnes. Certains programmes d'IDN s'appuient sur la technologie Blockchain tandis qu'un nombre croissant d'entre eux utilisent des données biométriques telles que les empreintes digitales ou la reconnaissance vocale et faciale. Plusieurs gouvernements jouent un rôle important en tant que garants des programmes d'IDN, l'Asie du Sud-Est étant la région la plus avancée sur le sujet. Cinq des dix pays de l'association ASEAN, à savoir l'État de Brunei, l'Indonésie, la Malaisie, Singapour et la Thaïlande, exploitent déjà des réseaux publics d'IDN, les autres nations étant en train de leur emboîter le pas.

Appliqués à la prévention de la criminalité financière, de tels programmes peuvent avoir un impact important sur les processus d'obligation de vigilance à l'égard de la clientèle et de connaissance des clients. En effet, ils permettent aux établissements financiers de rendre l'identification de nouveaux clients plus facile, et donc potentiellement moins coûteuse, plus rapide et plus fiable, le tout à partir d'une source fiable au moment de l'intégration. En outre, la technologie IDN peut atténuer le risque de fraude au-delà de l'intégration, des données d'identification pouvant être requises pour accéder à et utiliser des comptes de manière continue.

Bien entendu, une technologie aussi récente n'est pas dénuée de risques car il est tout à fait possible de concevoir des IDN synthétiques à partir d'informations réelles et falsifiées et de les ajouter au réseau, surtout avec la complicité de personnes en interne. Comme pour tout système basé sur des données, la sécurité et la gouvernance du réseau sont essentielles à sa crédibilité, d'où le rôle que de nombreux gouvernements et établissements d'envergure jouent dans son développement. Si l'on veut que les IDN aient l'effet escompté, il sera donc essentiel que toutes les parties prenantes aient confiance dans les fondements et les protections mises en place.



Gestion intégrée des risques

L'intégration en interne des structures de gestion des risques de criminalité financière est une autre nouvelle tendance qui devrait se poursuivre et se renforcer en 2020. Dans de nombreux grands établissements financiers, le processus a généralement été enclenché en associant des fonctions de lutte contre le blanchiment et la fraude ainsi que d'autres domaines liés à la gestion des risques de criminalité financière, par exemple le financement du terrorisme, les sanctions, la corruption et les pots-de-vin, sans oublier la cybersécurité qui a des points de contact naturels avec des crimes sous-jacents tels que la fraude en ligne.

Une grande partie de cette activité est le fait d'établissements financiers plus importants, souvent après l'adoption de mesures réglementaires et alors qu'il était urgent d'établir des liens entre des types de risques interconnectés et de promouvoir une culture proactive en matière de risque de criminalité financière. L'intégration plus étroite d'équipes d'enquêteurs qui analysent les alertes remontées par les systèmes LCB et de filtrage est une parfaite illustration d'une initiative concertée. D'autres établissements ont également adopté une approche « latérale » en transmettant directement les alertes issues de la supervision des transactions aux chargés de relations afin que soient rapidement prévenus ceux qui connaissent bien les comptes clients.

Ces changements ont un impact positif, mais s'ils ne sont pas traités avec tact, ils peuvent aussi être une source de tensions importantes. Lorsque des fonctions et des missions bien distinctes sont en place depuis longtemps, associer différents personnels, systèmes et procédures peut avoir un effet contreproductif pendant un certain temps. Par conséquent, les entreprises les mieux placées pour tirer parti d'une approche intégrée sont encore une fois celles qui sont plus jeunes et plus agiles, d'autant plus qu'elles sont également les mieux placées pour aligner cette approche sur l'évolution de leurs solutions technologiques intégrées.

Les partenariats public–privé (PPP)

On retrouve l'intégration interne opérée au sein des établissements financiers dans la relation entre le secteur privé et les autorités chargées de faire appliquer la loi et la réglementation et qui appartiennent donc au secteur public. Depuis un certain temps déjà, le gouvernement américain encourage le secteur privé à coopérer en fournissant des renseignements financiers. En effet, la section 314(b) de la loi PATRIOT de 2001 offre aux établissements financiers américains le cadre juridique nécessaire pour partager des informations entre eux au sein d'une « sphère de sécurité » dégagée de toute responsabilité et qui permet d'identifier et de signaler les risques LCB/FT. Plus récemment, la tendance est à la participation plus directe de l'État par le biais de partenariats public–privé (PPP). De tels partenariats permettent un partage volontaire d'informations entre le secteur public et le secteur privé dans les limites des lois existantes, à savoir des informations sur les tendances et les typologies ainsi que des informations tactiques dans certains cas.

L'un des partenariats PPP parmi les plus connus est le Joint Money Laundering Intelligence Task Force (JMLIT) créé au Royaume–Uni en 2015. Cependant, depuis 2015, des initiatives du même genre ont été lancées en Australie (Fintel Alliance), aux États–Unis (l'organisme FinCEN) et au Canada (le Projet PROTECT) tandis que d'autres projets n'en sont qu'à leurs débuts en Irlande et en Nouvelle–Zélande. Les principaux centres financiers d'Asie de l'Est ont également mis en place des initiatives similaires dont le partenariat de l'industrie de la lutte contre le blanchiment et le financement du terrorisme (ACIP) à Singapour et le Groupe de travail sur le renseignement en matière de fraude et de blanchiment (FMLIT) à Hong Kong. En Europe, Europol a développé son propre partenariat public–privé en matière de renseignement financier avec l'EFIPPP, sachant que le développement de partenariats PPP au niveau national prendra un peu plus de temps. Le plus important à ce jour est la task force néerlandaise de lutte contre le financement du terrorisme baptisée TF Taskforce. L'Allemagne a quant à elle annoncé la création de sa propre initiative en octobre 2019, l'Alliance contre la criminalité financière (AFCA), tandis que la Suède et le Danemark envisageraient d'en faire de même.

L'un des points de friction entre plusieurs juridictions européennes concerne la réglementation sur la protection des données. En effet, en vertu du Règlement Général sur la Protection des Données (RGPD) de l'UE entré en vigueur fin mai 2018, l'article 23 invoque des raisons d'« intérêt public » pour autoriser le partage de données sans le consentement de la personne concernée, sachant que la définition de l'« intérêt public » est sujette à discussion. La situation devrait continuer d'évoluer positivement dans de nombreux pays européens, mais avec prudence.

De nouveaux progrès verront le jour en Europe principalement parce que les PPP ont un réel impact positif sur la criminalité financière. Les déclarations d'activités suspectes (DAS) générées suite au partage d'informations seraient plus pertinentes et de meilleure qualité que celles produites sans contexte. Néanmoins, la prochaine grande question concernant les PPP est celle de leur évolutivité. Les partisans des PPP ont insisté pour savoir ce qu'on attend précisément d'eux dans la mesure où le volume de cas qu'ils peuvent traiter actuellement est relativement faible. Au niveau du droit, de l'infrastructure et des ressources en jeu, une solution « progressive » permettant d'échanger des informations en temps réel représenterait un chantier considérable. À moins d'une évolution radicale du public concernant la protection des données et d'une modification de la législation en la matière, il est probable que ce sont les technologies qui renforcent la protection de la vie privée (PET) qui seront le plus massivement sollicitées pour faciliter le partage d'informations. Tout le potentiel de ces technologies a été démontré à l'occasion du salon Tech Sprint UK 2019, sachant que ces dernières sont encore immatures et potentiellement contestables sur le plan juridique. Et même une fois ces problèmes surmontés, les organismes chargés d'appliquer la loi auront besoin, et ce n'est pas une nouveauté, d'un plus grand pouvoir d'investigation pour enquêter et exploiter des pistes à la fois nouvelles et de meilleure qualité.

L'autre défi de taille concerne la légitimité. En effet, dans la plupart des cas, les PPP sont dominés par les banques. L'ampleur et l'ancienneté de l'établissement semblent être des facteurs déterminants pour participer à l'initiative. Ainsi, au Royaume–Uni, les FinTechs liées à la task force JMLIT participent principalement à des forums de discussion d'ordre général en rapport avec l'initiative PPP. La raison qui est actuellement avancée pour expliquer pourquoi les FinTechs sont évincées du partage d'informations plus opérationnelles est qu'elles ne disposent pas de la capacité transactionnelle ou de l'expérience d'investigation des banques institutionnelles. Toutefois, cet argument commence à perdre en crédibilité compte tenu de l'importance croissante des banques concurrentes, des fournisseurs de paiements sur mesure et des méthodes de paiement alternatives telles que les actifs virtuels. Les FinTechs devraient donc être, espérons–le, plus nombreuses à frapper à la porte des PPP en 2020 afin de pouvoir participer en plus grand nombre à cette initiative.

Quelles conséquences pour mon entreprise ?

- Chaque établissement financier devrait s'intéresser à la façon de déployer une technologie RegTech innovante. Un volume gigantesque de données ouvertes et pertinentes permet désormais d'évaluer les risques et est à la disposition des entreprises du secteur financier comme le soulignent les autorités réglementaires. Toutefois, sans recourir à une technologie qui évolue, il est presque impossible pour les établissements financiers d'examiner ces données et de les exploiter de manière ponctuelle et productive.
- Dans la mesure du possible, les établissements financiers devraient donc chercher à déployer des solutions intégrées aussi bien pour la lutte contre le blanchiment que pour leurs obligations de vigilance à l'égard de la clientèle ou la supervision des transactions, ceci afin d'avoir une « vue à 360 degrés » du client.
- Les établissements financiers devraient envisager de s'appuyer sur l'IDN tout en atténuant les risques liés à la sécurité des données et à la protection de la vie privée dans un souci premier d'efficacité.
- Ces mêmes établissements devraient élaborer des moyens d'intégrer des fonctions de gestion des risques apparentées, mais pas au prix d'une rupture de leurs capacités opérationnelles actuelles. Alors que les FinTechs peuvent intervenir rapidement dans ce domaine, les établissements financiers institutionnels doivent faire preuve de prudence.
- Les établissements financiers devraient chercher à s'impliquer dans des PPP pertinents et dans des structures de partage d'informations pilotées par l'industrie.

Les tendances à venir du marché

Comme à bien d'autres égards, les initiatives les plus intéressantes se concrétiseront dans le secteur de la FinTech en 2020. Malgré certaines informations faisant état d'une bulle FinTech sur le point d'éclater, les bases du secteur restent solides. Selon le site Web Statista qui publie des aperçus et des données pour 600 secteurs et plus de 50 pays, la valeur des paiements numériques à l'échelle mondiale augmente actuellement à un rythme de 12,8 %. Dans de nombreux pays soutenant ouvertement la FinTech, des start-ups relativement jeunes concurrencent déjà sérieusement les établissements financiers en place depuis longtemps. Au Royaume-Uni, Monzo, Revolut et Starling Bank consolident leur position vis-à-vis des banques de détail plus anciennes. Aux États-Unis et en Europe, une poignée de FinTechs parmi lesquelles Varo Money et N26 ont sollicité et obtenu des chartes bancaires. Dans la région Asie-Pacifique aussi, le secteur est stimulé par un nombre toujours plus important d'autorités qui délivrent des licences bancaires numériques (DBL) aux « néo-banques ». En 2019, Hong Kong, Singapour et Taiwan ont déjà émis un petit nombre de licences DBL et en émettront probablement davantage au cours de cette année. La Thaïlande et la Malaisie envisagent de faire de même. Dans d'autres pays, FinTechs et établissements bancaires traditionnels trouvent un terrain d'entente pour s'associer plutôt que de se faire concurrence. Une étude réalisée en 2019 par Bank Innovation, une agence de presse américaine en ligne dédiée à la FinTech, et par INV Fintech, un accélérateur de start-ups, a révélé que 43 % des établissements financiers estimaient avoir profité de leur collaboration avec des FinTechs tandis que 77 % des établissements interrogés ont déclaré qu'ils prévoyaient de s'impliquer dans des collaborations de même nature en 2020 et 2021.

Néanmoins, même si les fondamentaux commerciaux du marché sont solides, les FinTechs doivent encore relever le défi de la conformité. L'enquête de Bank Innovation a révélé que le principal obstacle à la collaboration entre FinTechs et grands établissements financiers était le manque de sécurité des données et de conformité réglementaire des premières. Même si de nombreuses FinTechs sont en train de trouver des solutions à ces problèmes, certaines ne le font pas tandis que d'autres suivent par réflexe les modèles existants des grandes banques pour se protéger contre l'œil inquisiteur du régulateur. Aucune de ces deux approches, que ce soit la politique de l'autruche ou une assurance excessive, ne pourra fonctionner. L'une favorise l'action réglementaire tandis que l'autre conduit à une escalade des coûts de conformité et à une efficacité médiocre. Des enquêtes du secteur bancaire publiées en 2019 ont indiqué que, même si le rythme auquel les coûts de conformité augmentent pourrait ralentir, les budgets et les effectifs restent obstinément élevés.

Ce qui est déjà un problème pour les établissements financiers institutionnels ne doit pas forcément l'être aussi pour les FinTechs. Comme évoqué plus haut, la réalité du marché oriente fortement vers un déploiement de la RegTech plus intégré, imaginatif et agile afin de réduire les coûts et de mieux cerner les risques de criminalité financière. Cela sera probablement plus facile pour les FinTechs que pour les établissements financiers traditionnels et l'attitude actuelle du régulateur envers l'innovation technologique est le meilleur moyen pour que tout se passe pour le mieux. Comme indiqué plus haut aussi, un nombre croissant de FinTechs s'engagent avec des partenaires RegTech pour exploiter les opportunités qu'offrent les « bacs à sable réglementaires ». En mai 2019, Onfido, la RegTech de vérification d'identité, annonçait une collaboration avec des FinTechs comme Monese et Curve pour tester une solution de vérification d'identité en ligne plus fiable dans la cinquième cohorte du « bac à sable réglementaire » de la FCA, l'autorité de bonne conduite financière britannique. Logique sur le plan du marché et de la réglementation, nous nous attendons à ce que ce genre d'engagement et de collaboration se multiplie dans tout le secteur au cours de cette année.

Quelles conséquences pour mon entreprise ?

- Que vous soyez une banque ou une FinTech, voyez au-delà de votre entreprise.
- Demandez-vous comment collaborer avec des RegTechs peut vous aider à mieux atténuer vos risques en matière de criminalité financière
- Avez-vous la possibilité de tirer parti du savoir-faire d'autres entreprises au moyen d'un partenariat ?
- Vous devez respecter les règles par principe, mais votre responsabilité vis-à-vis du marché au sens large et de vos clients vous oblige aussi à lutter contre la criminalité financière. La meilleure façon d'y parvenir est de travailler avec les autres.

Moments forts en 2020

1er/2ème trimestre

Examen par le Sénat américain du projet de loi SAFE Banking Act

28 janvier

Singapour – Entrée en vigueur de la Loi sur les services de paiement (PSA Act)

Février

Publication des évaluations mutuelles du GAFI : Corée du Sud et Émirats Arabes Unis

10 mars

Entrée en vigueur des registres de la propriété effective des trusts (UE)

9 mai

Date de renouvellement des ordonnances de ciblage géographique (GTO) du FinCEN sur les marchés immobiliers métropolitains américains

Juin

Évaluations mutuelles du GAFI : Japon et Afrique du Sud

Examen par le GAFI de l'application de la « règle de voyage »

10 janvier

Transposition de la 5ème Directive LCB (5AMLD) de l'UE dans le droit des États membres
Entrée en vigueur des registres de la propriété effective des entreprises (UE)

31 janvier

Le Royaume-Uni quitte l'UE ; début de la période de transition et négociations sur les futures relations avec l'UE

Mars

Évaluations mutuelles du GAFI : Tanzanie

Mai

Évaluations mutuelles du GAFI : Sierra Leone, Sainte-Lucie et Venezuela

Milieu d'année

Annonce des nouvelles licences bancaires numériques (DBL) de Singapour

Moments forts en 2020

1er juin

Canada — Entrée en vigueur de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes

Août

FATF Évaluations mutuelles du GAFI : Mozambique

10 septembre

Entrée en vigueur de mécanismes automatisés et centralisés pour identifier les personnes détenant ou contrôlant des comptes de paiement et des comptes bancaires (UE))

Novembre

Évaluations mutuelles du GAFI :
Égypte, Dominique, Togo et Niger

Décembre

Évaluations mutuelles du GAFI : Saint-Marin, Bolivie et le Saint-Siège

31 décembre

Fin de la période de transition du Brexit britannique

Juillet

Évaluations mutuelles du GAFI : République slovaque, Géorgie, Chili, Vietnam et Tonga

Septembre

Évaluations mutuelles du GAFI : Tchad

Octobre

Évaluations mutuelles du GAFI : Nouvelle Zélande

3 novembre

Election présidentielle américaine

3 décembre

Transposition de la 6ème Directive LCB (6AMLD) de l'UE dans le droit des États membres de l'UE

09

À propos de ComplyAdvantage

La vision de ComplyAdvantage est d'identifier et neutraliser le risque de blanchiment d'argent, de financement du terrorisme, de corruption et de tout autres crimes financiers mondiaux en fournissant la seule base de données mondiale dynamique sur les risques des personnes et des entreprises. ComplyAdvantage s'intègre de manière transparente grâce à une suite de solutions cloud configurables, pour aider à automatiser et à réduire la frustration liée au respect des sanctions, de la lutte contre le blanchiment d'argent et des réglementations LCB/FT.

Fondée en 2014, ComplyAdvantage travaille avec plus de 500 entreprises dans 75 pays. Soutenue par Index Ventures et Balderton Capital, ComplyAdvantage dispose de quatre hubs mondiaux à Londres, New York, Cluj-Napoca et Singapour. Pour plus d'informations, rendez-vous sur:

complyadvantage.com/fr

Nos clients

LEMONWAY robinhood earthport Munich RE Santander

Contactez-nous

EMEA
Londres

+44 20 7834 0252
contact.uk@complyadvantage.com

AMER
New York

+1 (646) 844 0841
contact.usa@complyadvantage.com

APAC
Singapour

+65 6304 3069
contact.sg@complyadvantage.com