COMPLY ADVANTAGE®

L'état de la criminalité financière en 2023

Coup de projecteur sur la criminalité financière

Contenu

Introduction

Andrew Davies
Responsable mondial des affaires réglementaires chez ComplyAdvantage

Alors que 2023 était censée être l'année pour nous rétablir des ondes de choc de la pandémie de Covid-19, l'enquête que nous publions cette année démontre clairement que ce ne sera pas le cas.

En effet, la crise économique mondiale déclenchée par les effets inflationnistes du « retour à la normale » et la guerre en Ukraine ont incité 99 % des répondants à nous dire qu'ils allaient réviser leur appétit pour le risque en 2023. Réjouissons-nous cependant que 58 % des équipes chargées de la conformité dans les établissements financiers prévoient d'embaucher en 2023 pour relever ce défi. De plus, la plupart des personnes interrogées ont démontré qu'elles savaient que la prévention et la gestion des risques de criminalité financière ne se résumaient pas à embaucher du personnel supplémentaire. En effet, la technologie et la transformation organisationnelle sont également indispensables. À noter aussi que l'inclusion financière pourrait être gravement impactée si les établissements ne s'appuient pas sur une technologie qui optimise le processus d'entrée en relation d'affaires en fonction d'un appétit pour le risque repensé.

Notre rapport met en lumière d'autres problèmes majeurs comme le financement de groupes terroristes par le biais de plateformes décentralisées avec des tendances anciennes qui se sont accélérées au cours de la pandémie. La criminalité environnementale est un autre sujet important avec la montée en flèche des crimes, notamment le braconnage et l'exploitation forestière illégale.

L'invasion de l'Ukraine et son impact mondial durable restent une autre préoccupation majeure en ce début d'année 2023. Sans surprise, la Russie est devenue le point chaud géopolitique qui inquiète le plus les établissements financiers, plus encore que la Chine. Sans perspective de résolution, l'accent sera mis sur un régime de sanctions sans précédent qui pourrait devenir un modèle pour les crises à venir. Pour l'heure, les sanctions à l'encontre de la Russie devraient encore se durcir en 2023, malgré la pression intense à laquelle sont confrontés de nombreux pays occidentaux en raison de la hausse vertigineuse de leurs factures énergétiques et alimentaires. En outre, une attention accrue sera certainement portée sur les points chauds traditionnels que sont la Corée du Nord et l'Iran.

Au niveau réglementaire, nous devrions bientôt pouvoir apprécier les premiers résultats de la présidence singapourienne du Groupe d'action financière (GAFI) avec le recouvrement des avoirs qui est un dispositif-clé. Aux États-Unis, nous assisterons à une réforme réglementaire majeure du marché des crypto-actifs, même s'il reste à statuer sur de nombreux points. La Chine et Singapour ont également fait d'importants progrès concernant la réglementation des fournisseurs de services d'actifs virtuels. En parallèle, le programme permanent de réforme de la lutte contre le blanchiment d'argent (LCB) de l'Union européenne (UE) devrait évoluer vers une loi avec la création dans la foulée d'une nouvelle autorité européenne de lutte contre le blanchiment (AMLA) en Europe.

Quant à la dernière section de notre rapport, elle s'intéressera aux tendances et sujets plus généraux du secteur. Cette année, nous nous pencherons sur l'intérêt porté à la propriété effective et à la transparence des entreprises ainsi que sur l'importance que cela revêt pour comprendre des facteurs comme l'origine des fonds, la corruption et l'évasion fiscale. Certains établissements nous ont par ailleurs indiqué les cas d'utilisation de l'intelligence artificielle (IA) qui ajoutent le plus de valeur à leurs activités. Enfin, les initiatives en matière de connaissance des clients (KYB) et de gouvernance environnementale et sociale (ESG) occuperont le devant de la scène en 2023. Nous détaillerons les implications pratiques de cette évolution pour la communauté de la conformité.

Les enjeux sont absolument majeurs, qu'il s'agisse d'une guerre bien ancrée en Europe ou de l'environnement économique mondial le plus instable depuis plus d'une décennie. Les défis auxquels sont confrontés les professionnels de la conformité n'ont certainement jamais été aussi complexes. Et pourtant, je reste optimiste. Les outils, les technologies et les recommandations à la disposition des établissements sont meilleurs que jamais, ce qui permet de lutter plus efficacement contre la criminalité financière et, au final, de garantir un monde meilleur pour toutes et tous.

Nous espérons que vous apprécierez de lire ce rapport autant que nous avons eu de plaisir à le rédiger.

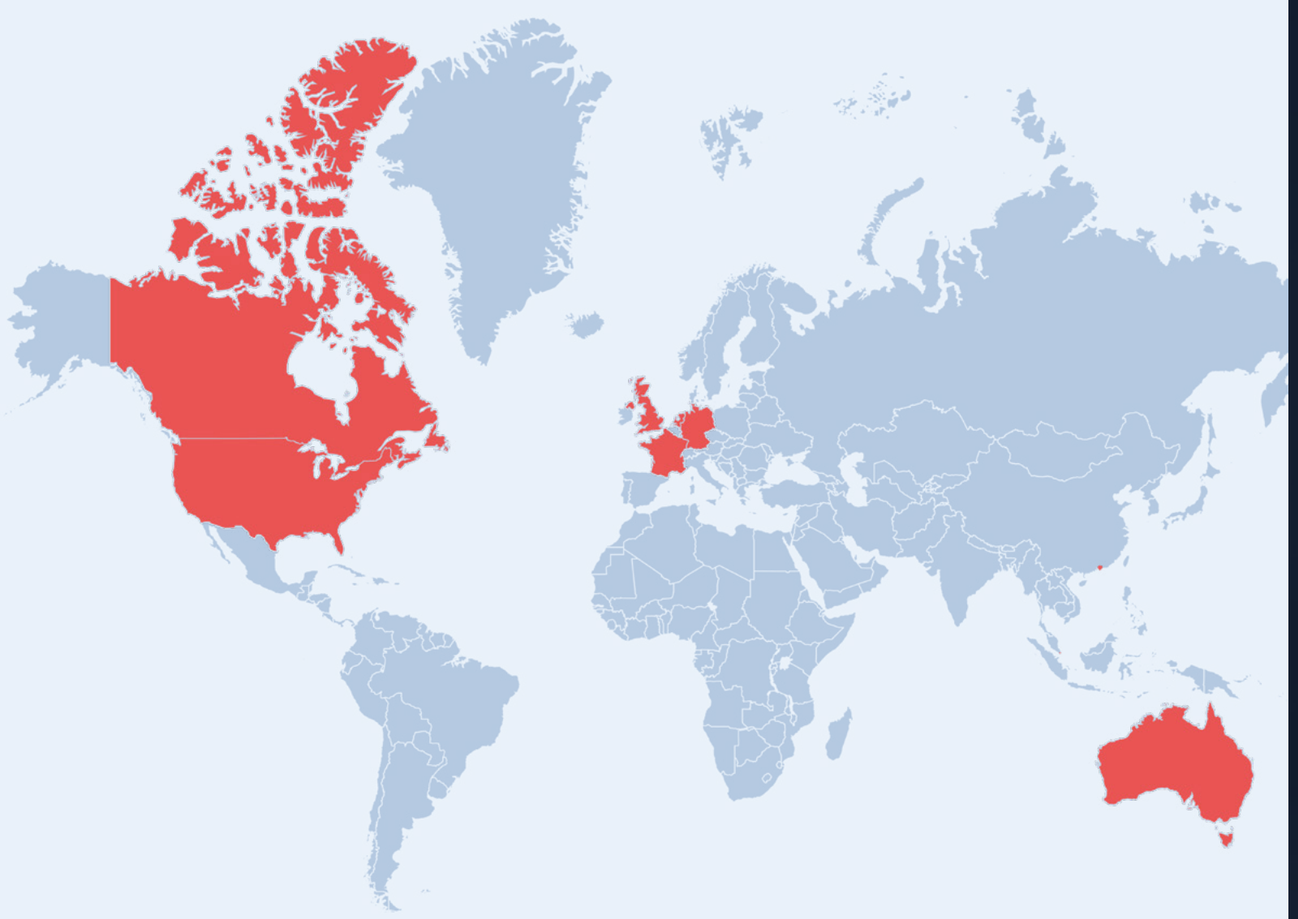
Bien cordialement,

Méthodologie

Ce rapport s'appuie sur une enquête menée auprès de 800 décideurs dans le domaine de la conformité (cadres et hauts dirigeants) exerçant aux États-Unis, au Canada, au Royaume-Uni, en France, en Allemagne, aux Pays-Bas, à Singapour, à Hong Kong et en Australie.

Tous les répondants travaillent actuellement dans des entreprises de services financiers et des FinTechs qui comptent plus de 50 employés et ont plus de 5 milliards de dollars d'actifs.

Ces entretiens portent sur l'activité des établissements financiers (banques,...), la banque numérique et les FinTechs, la gestion de patrimoine, l'investissement (grand public), les marchés de capitaux, les prestataires de services monétaires, les bourses de crypto-monnaies et les assurances.



Coup de projecteur sur la criminalité financière

Cette section s'intéresse aux tendances qui façonnent le paysage financier actuel et à leurs implications pour l'année qui commence. Comme l'indique notre enquête, les entreprises se préparent à affronter en 2023 une augmentation de la criminalité financière en se dotant de personnel supplémentaire tout en repensant leur approche du risque.

Cependant, le changement qui a suscité le plus de commentaires - et qui a eu l'impact le plus important sur les entités soumises à l'obligation - a été l'introduction de l'infraction de « complicité ». Il s'agit d'une tentative de dissuader la croissance du marché des facilitateurs professionnels du blanchiment d'argent dans le secteur des services juridiques, comptables et professionnels, mais aussi parmi les membres de la famille, les proches et les collaborateurs des criminels qui ont joué le rôle de mandataires dans des systèmes de blanchiment complexes. En termes pratiques, l'infraction de « complicité » signifie que toute personne - y compris les entreprises et les particuliers - qui aide les blanchisseurs de capitaux à dissimuler des fonds peut elle-même commettre le crime de blanchiment de capitaux. Cependant, comme de nombreux acteurs du secteur l'ont demandé au moment de l'introduction de la directive, la signification pratique de l'application de la notion de « complicité » n'était pas claire. Lorsqu'un conseiller ou une institution financière avait explicitement su, ou même supposé, que des fonds étaient criminels, il n'y avait aucune raison de s'inquiéter. Mais qu'en est-il des « actes d'omission » ? Le risque existe que des manquements prolongés et non intentionnels à la conformité, permettant à des criminels de blanchir des fonds, soient considérés comme un acte criminel, ainsi que comme une défaillance réglementaire nécessitant des mesures d'application.

La volatilité économique redéfinit les comportements à l'égard du risque

En 2023, le ralentissement économique mondial va perturber l'espace de la criminalité financière et de la conformité. Alors que certains avaient prédit des « années folles » avec la réouverture d'une grande partie du monde et avec la « Grande Démission » qui a redéfini l'environnement de travail, la réalité est bien différente.

97 % des entreprises en France nous ont déclaré réévaluer leur appétit pour le risque en raison de l'environnement économique. Cette approche plus conservatrice, ainsi que l'obligation de vigilance raisonnable renforcée à l'égard de la clientèle que cela exigera, vont accentuer la pression sur les aspirations à simplifier et faciliter l'accès aux services financiers. Pour répondre à cette demande tout en gérant un appétit plus prononcé pour le risque, il faudra investir à la fois dans la technologie et dans du personnel.

La prudence du secteur est motivée par la crainte que, comme lors des précédents ralentissements économiques, les niveaux de criminalité financière augmentent. Cette augmentation pourrait ne pas être uniquement liée aux criminels professionnels endurcis.

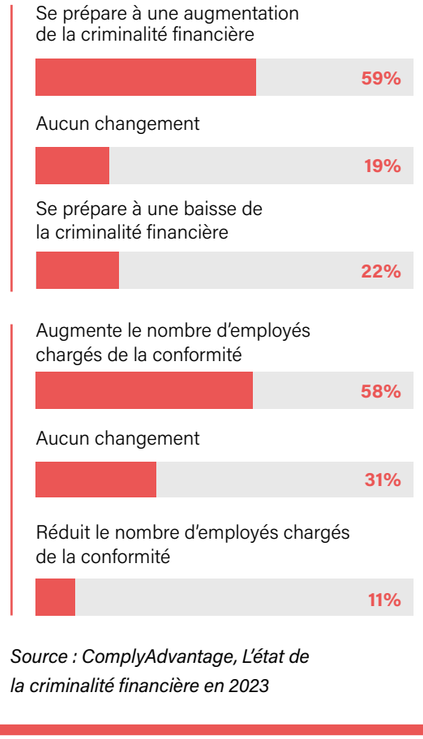
En effet, la pression économique pourrait entraîner une hausse plus importante des comportements à risque de la part d'acteurs auparavant légitimes, certains franchissant la ligne rouge de la criminalité financière. L'Autorité de bonne conduite financière britannique (FCA) a également prévenu que l'augmentation du coût de la vie conduira les criminels à exploiter le public par le biais de fraudes aux frais de prêt et d'escroqueries au paiement anticipé autorisé. À noter aussi que certains établissements nous ont indiqué avoir communiqué plus de rapports d'activités suspectes (SAR) en 2022 qu'en 2021. 78 % des répondants résidants en France ont déclaré en avoir déposé davantage, soit une hausse de 9 % du nombre d'établissements nous ayant déclaré en avoir signalé davantage en 2020 qu'en 2019. Tout cela indique que le volume et la variété des délits financiers que les établissements signalent aux autorités augmentent avant même que la pression d'un ralentissement économique ne se fasse sentir.

97 %

des professionnels français de la conformité réévaluent leur approche au risque.

Source : ComplyAdvantage, L'état de la criminalité financière en 2023

Parmi les éléments suivants, comment votre équipe de conformité répond-elle à l'incertitude de l'environnement économique en France ?



Source : ComplyAdvantage, L'état de la criminalité financière en 2023

Les perspectives économiques sombres n'empêchent pas les professionnels de la conformité de faire preuve de réalisme. 49 % des répondants français sont prêts à faire face à une augmentation de la criminalité financière tandis que 62 % prévoient d'embaucher du personnel supplémentaire. Même si les taux de chômage devraient augmenter, seulement 10 % des entreprises en France prévoient de réduire le volume de leur personnel chargé de la conformité.

A contrario, le marché de l'emploi du personnel de conformité est susceptible de s'emballer. Cela pourrait être dû en grande partie à la croissance des « super applications ». Déjà populaires en Orient grâce à WeChat, Alipay et autres, l'essor d'applications semblables en Occident contraindra des entreprises comme Meta, Twitter et Snap, qui lorgnent sur cette opportunité, à embaucher rapidement. Tout en offrant plus de confort aux consommateurs, ces super applications créent aussi des espaces dans lesquels les criminels peuvent s'engouffrer et partager des informations. Cela pourrait entraîner une augmentation des typologies de fraude telles que les prises de contrôle de comptes, la fraude aux paiements et des abus liés aux systèmes de recommandation.

Quelles conséquences pour mon entreprise ?

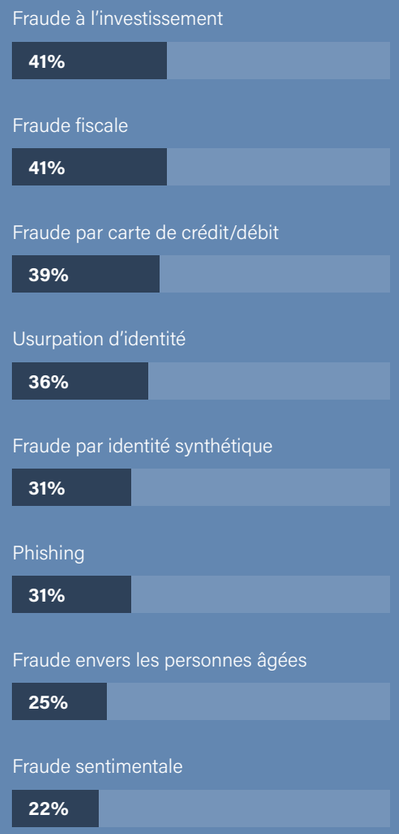
« Associé à l'adoption croissante de nouvelles technologies, le ralentissement économique offre un terreau fertile pour de nouvelles typologies de criminalité financière. Ainsi, dans le domaine de la fraude, de plus en plus d'établissements financiers vont devoir rembourser les victimes sans pouvoir le leur reprocher. Ces établissements chercheront donc, autant que possible, à réaliser davantage de profits tout au long du cycle de vie de la fraude afin de réduire les coûts liés à ces remboursements. Déjà appliquée dans certains établissements, l'interdiction du suivi des flux de fonds en temps réel sera de plus en plus répandue pour limiter la responsabilité tout en protégeant la clientèle.

En parallèle, au moment de l'entrée en relation d'affaires, les établissements souhaiteront renforcer leur capacité à évaluer les risques des clients et se donner toutes les chances d'éviter d'intégrer des criminels. Les plateformes unifiées dédiés à la connaissance initiale et permanente de la clientèle (KYC) seront prisées et renforcées par des outils d'identification et de vérification (ID&V) plus performants. Il reste difficile pour les établissements financiers de trouver un équilibre entre la préférence des clients pour un processus d'entrée en relation d'affaires et de suivi des opérations courantes à la fois simple et direct et la nécessité de se protéger contre les activités criminelles. Les initiatives en matière d'identité numérique soutenues par l'État, notamment les portefeuilles EUDI de l'Union européenne et le règlement eIDAS 2.0, au cœur de l'EUDI, peuvent apporter une réponse. Toutefois, les tentatives précédentes pour atteindre des objectifs similaires ont été entachées par un manque d'adhésion et des opinions divergentes entre les gouvernements nationaux concernant les moyens les plus efficaces de déployer et de maintenir un tel système. »

Iain Armstrong
spécialiste des affaires réglementaires chez ComplyAdvantage

La fraude et les escroqueries continuent d'évoluer

Quels sont les types de fraude qui préoccupent le plus votre entreprise ?



Source : ComplyAdvantage, L'état de la criminalité financière en 2023

Alors que les inquiétudes en matière de fraude ont atteint leur paroxysme pendant la pandémie en raison des abus vis-à-vis des plans d'aide et de relance, on ne sait toujours pas dans quelle mesure les criminels ont profité de ces programmes. Par exemple, APT41, un acteur malveillant bien connu qui entretient des liens avec le gouvernement chinois, aurait dérobé des **dizaines de millions de dollars de prestations d'aide destinées à lutter contre le Covid**. Alors que les gouvernements européens mettent en place des mesures de relance pour compenser la hausse des factures d'énergie et que les **États-Unis approuvent un programme de subventions de l'énergie verte de 430 milliards de dollars**, 2023 devrait être marquée par un regain d'intérêt pour la fraude aux mesures de relance et aux subventions gouvernementales.

Les données de notre enquête indiquent que la fraude fiscale et la fraude à l'investissement sont les deux principales préoccupations des professionnels de la conformité pour 2023. Si toutes deux sont probablement alimentées par le ralentissement économique, la fraude à l'investissement, en particulier, est souvent anticyclique par rapport à l'économie. À mesure que l'accès au financement se complique, la tentation de recourir à de faux programmes offrant des rendements apparemment « supérieurs à ceux du marché » augmente. Les statistiques de la Commission américaine de détermination des peines montrent que si le nombre d'auteurs de fraudes aux valeurs mobilières et aux investissements a diminué au cours des cinq dernières années, la **perte moyenne a grimpé en flèche pour atteindre plus de 2 880 000 dollars**. En août 2022, la Commission des opérations en bourse (SEC) a également publié des recommandations sur l'utilisation croissante des plateformes de médias sociaux pour obtenir des conseils en matière d'investissement. Elle déclare que « les fraudeurs peuvent configurer un nom de compte, un profil ou un identifiant pour imiter un individu ou une entreprise en particulier. Ils peuvent aller jusqu'à créer une page Web qui reprend le logo de l'entreprise légitime, des liens vers le site Web de cette dernière ou encore mentionner le nom d'une personne travaillant pour cette même entreprise. En outre, les fraudeurs peuvent orienter des investisseurs vers un site Web frauduleux en publiant sur des comptes de médias sociaux des commentaires de courtiers, de conseillers en investissement ou issus d'autres sources d'informations sur le marché. »

La fraude par carte de crédit et de débit reste une préoccupation majeure pour 45% des répondants résidants en France. Une bonne partie de cette fraude s'appuie sur le commerce électronique, les achats effectués par téléphone, par Internet ou par correspondance à l'aide de cartes volées étant estimés à plus de 10 milliards de dollars d'ici 2024. La popularité des cartes de crédit pour réaliser des achats en ligne fait qu'elles représentent une part importante de cette fraude.

Les typologies émergentes telles que la fraude à l'identité synthétique occupent aussi une place importante et préoccupent même davantage que la fraude en lien avec les personnes âgées et les histoires de cœur. KPMG cite la fraude à l'identité synthétique comme étant le crime financier à la croissance la plus rapide aux États-Unis et qui coûte plus de 6 milliards de dollars aux banques. En 2023, la fraude à l'identité synthétique devrait continuer d'augmenter avec des criminels qui trouvent de nouveaux moyens d'abuser des consommateurs en raison de la pression économique actuelle. La fraude hypothécaire en est un exemple. Alors que la hausse des taux d'intérêt fait grimper le coût des prêts hypothécaires dans de nombreux pays, les personnes qui cherchent désespérément à obtenir un financement pourraient s'intéresser à des technologies plus évoluées et de plus en plus accessibles pour contourner les exigences de plus en plus strictes concernant les prêteurs.

2023 devrait aussi être l'année où davantage d'entreprises se lancent dans le métavers. Par conséquent, les criminels seront eux aussi plus nombreux à s'y intéresser. C'est ainsi que l'on estime qu'une personne sur quatre passera au moins une heure par jour dans le métavers d'ici 2026. En partenariat avec INTERPOL, Meta, Microsoft et d'autres, le Forum économique mondial a prévenu que les escroqueries s'appuyant sur l'ingénierie sociale, l'extrémisme et la désinformation figureront probablement parmi les principaux défis à relever. Reconnaissant que le métavers est « déjà là » INTERPOL a également lancé son propre métavers et fait visiter son siège aux utilisateurs tout en leur permettant d'interagir avec d'autres agents et de suivre des formations. Avec des analystes qui prévoient une économie virtuelle dans le métavers qui sera facilitée par les monnaies virtuelles et les jetons non fongibles (NFT), les risques de criminalité financière associés aux cryptomonnaies sont également susceptibles d'entrer en collision avec les nouvelles réalités virtuelles. Selon Morgan Stanley, les risques concernent notamment des manipulations du prix des NFT ainsi que des jetons NFT contrefaits et malveillants.

Ces problèmes de fraude sont aggravés par l'essor continu du commerce électronique, dont les ventes mondiales devraient augmenter de 56 % d'ici à 2026 pour atteindre 8100 milliards de dollars. L'augmentation du volume du commerce électronique s'accompagne d'une volonté des fraudeurs d'exploiter les failles de ces plateformes. Les augmentations saisonnières de la demande créent aussi des pressions inégales tout au long de l'année avec des pics notamment à Noël.

Les débats sur l'efficacité et la responsabilité des autorités persisteront aussi tout au long de 2023. À Singapour, les chiffres de la police révèlent que le Centre anti-fraude a gelé plus de 7800 comptes bancaires et récupéré près de 80 millions de dollars au cours du premier semestre 2022. Toutefois, cela ne représente que 31 % du montant que les consommateurs ont perdu à cause d'escroqueries.

Il semblerait que le manque de confiance dans la capacité des forces de l'ordre à lutter contre la fraude n'incite pas toujours les victimes à porter plainte. En Australie, une enquête gouvernementale a montré que seulement 50 % des personnes victimes d'une escroquerie l'ont signalée.

Au France, le gouvernement s'est engagé à donner à l'organisme chargé de réglementer les systèmes de paiement les moyens d'obliger, dans certains cas, les entreprises à rembourser les victimes. Dans de nombreuses juridictions dont les États-Unis, la réglementation stipule toujours que si le consommateur autorise le transfert, l'établissement financier ne peut être tenu pour responsable tandis que le client peut être remboursé. Le secteur reconnaît l'importance de conserver la confiance des clients tout en s'inquiétant de l'impact de ces nouvelles recommandations sur des utilisations émergentes comme l'Open banking.

Quelles conséquences pour mon entreprise ?

« Les crimes financiers et la cybercriminalité sont inévitablement liés. En effet, pour chaque dollar fraudé, les établissements perdent près de trois dollars après avoir ajouté les coûts associés à la perte liée à la fraude elle-même. Dans un monde où les consommateurs interagissent essentiellement par le biais de canaux numériques, tout cela peut rapidement devenir coûteux pour les établissements concernés. Étant donné qu'une grande partie de la fraude financière s'appuie sur les technologies numériques, les fraudeurs recrutent des cybercriminels pour exploiter des technologies de paiement émergentes et blanchir ainsi leurs gains illicites tout en profitant des vulnérabilités inhérentes aux paiements en temps réel, à l'automatisation et à la dématérialisation. Avec un nombre d'utilisateurs du métavers qui augmente sans cesse et des technologies qui continueront de se développer, les services répressifs doivent faire eux-mêmes l'expérience du métavers. Pleinement opérationnel, le métavers d'INTERPOL permet aux utilisateurs enregistrés de visiter une copie virtuelle du siège du Secrétariat général d'INTERPOL basé à Lyon, sans aucune limite géographique ou physique, et d'interagir avec d'autres agents par l'intermédiaire de leur avatar. »

Alia Mahmud
spécialiste des affaires réglementaires chez ComplyAdvantage

Les activités liées au ransomware se diversifient

Les ransomware ne cessent de prendre de l'ampleur et des formes diverses. Une analyse publiée par le **réseau de lutte contre la criminalité financière (FinCEN)** précise que, par rapport à 2020, le nombre d'incidents liés aux ransomware qui ont été signalés au cours du second semestre 2021 a plus que doublé. Les déclarations en lien avec les ransomware effectuées dans la cadre de la loi sur le secret bancaire (BSA) ont représenté 1,2 milliard de dollars en 2021. En aout 2022, **le Centre hospitalier sud francilien (CHSF) de Corbeil-Essonnes** a été frappé par une cyberattaque, et le paiement d'une rançon s'élevant a 10 millions de dollars a été ordonnée par les cybercriminels en question. L'essentiel de l'augmentation des cybercriminels est dû aux différents variants de ransomware en lien avec la Russie, une tendance susceptible de s'accélérer alors que la Russie poursuit **sa cyber-guerre agressive dans le cadre de la guerre en Ukraine**.

2022 a également vu l'accélération de la convergence entre les ransomware et les cryptomonnaies, notamment via Deadbolt, un groupe qui s'attaque aux équipements et fournisseurs de stockage en réseau (NAS). Une clé de déchiffrement est envoyée automatiquement dès que le paiement de la rançon est effectué en bitcoin. Les infections par **Deadbolt** ont augmenté de 674 % rien qu'entre juin et septembre 2022, la plupart d'entre elles ayant été constatées aux États-Unis, en Allemagne et en Italie.

Les autorités de régulation ont pris des mesures pour informer et conseiller les entreprises rattachées à leurs juridictions sur la manière de lutter le plus efficacement possible contre les risques de ransomware. En avril 2022, le **Centre australien de rapports et d'analyse des transactions (AUSTRAC)** a publié un rapport signalant plusieurs indicateurs financiers en lien avec le ransomware, notamment l'augmentation rapide des limites de comptes clients et la découverte d'une photographie de données sur un écran d'ordinateur dans le cadre du processus de vérification du client lors de l'entrée en relation d'affaires. L'**Initiative internationale de lutte contre les ransomware (CRI)** a également organisé son deuxième sommet fin 2022 qui était consacré aux cyberattaques de grande envergure et au blanchiment via les monnaies numériques. Tout au long de 2023, cette structure s'attachera à mettre en place un groupe de travail sur les ransomware, à promouvoir l'engagement actif du secteur privé et à coordonner les principaux objectifs au moyen d'un cadre unique.

Outre la Russie, les auteurs d'attaques par ransomware parrainés par des États (Corée du Nord et Iran) sont devenus plus problématiques et le resteront. En avril, le Bureau de contrôle des actifs étrangers (OFAC) des États-Unis a étendu son régime de sanctions à des portefeuilles nord-coréens présumés suite au piratage du **réseau Ronin du jeu en ligne à base de blockchain Axie Infinity** qui a permis de dérober 600 millions de dollars de cryptomonnaies. En septembre 2022, **trois ressortissants iraniens** ont été accusés d'être derrière le piratage de plusieurs réseaux informatiques américains, y compris d'agences gouvernementales, d'organisations à but non lucratif et d'établissements de santé.

On ne sait pas exactement dans quelle mesure la **volatilité actuelle du marché des cryptomonnaies** affectera la préférence des acteurs du ransomware pour les cryptos comme méthode de paiement. Certains analystes ont fait valoir que les spécificités de la cryptomonnaie en font un moyen de paiement irremplaçable. D'autres ont souligné que les dévaluations contraindront les criminels à lancer des attaques plus fréquentes et plus agressives pour maintenir leur train de vie.

Quelles conséquences pour mon entreprise ?

« Les entreprises doivent revoir sans cesse leurs cyberdéfenses, leur hygiène des données ainsi que leurs programmes de formation pour s'adapter sans délai et le plus efficacement possible à l'évolution du paysage des ransomware. Il est essentiel de se familiariser avec les comportements les plus récents et toutes les formes spécifiques de ransomware qui ciblent leur secteur. En outre, il est indispensable d'examiner les toutes dernières recommandations des autorités de régulation opérant dans les juridictions concernées. En effet, elles vont continuer de publier des informations pratiques sur les risques auxquels les entreprises sont confrontées et sur les mesures qu'elles doivent prendre. Celles nées à l'ère du numérique qui n'ont pas encore déployé de programmes de « prime aux bogues » devraient envisager de le faire en complément d'exercices réguliers de test de pénétration. »

Iain Armstrong
spécialiste des affaires réglementaires chez ComplyAdvantage

Le trafic de stupéfiants déstabilise l'Amérique du Sud

De nouvelles preuves de l'ampleur considérable et croissante de la production de cocaïne à travers l'Amérique latine et de ses routes d'importation vers les États-Unis, l'Europe et la région Asie-Pacifique se sont accumulées tout au long de l'année 2022. L'Office des Nations unies contre la drogue et le crime (ONUDC) a publié des informations selon lesquelles la production mondiale est montée en flèche pour atteindre 1982 tonnes en 2020, en hausse de 11 % par rapport à 2019 et presque le double des niveaux de 2014. Une production croissante a également permis aux cartels de la drogue d'étendre leur influence dans toute la région, le Paraguay, l'Uruguay et le Chili ayant tous connu une hausse de la violence en lien avec la drogue en 2022. Les autorités du port d'Anvers ont quant à elles saisi plus de cocaïne en 2021 que tout autre grand port européen. Elles ont constaté que les trois principaux pays expéditeurs que sont l'Équateur, le Paraguay et le Panama ne sont pas de gros producteurs de drogue. L'ONUDC estime désormais que les 21 pays continentaux d'Amérique latine, à l'exception de trois d'entre eux, sont les « principaux pays par lesquels transite » la cocaïne. Le pouvoir et l'influence croissants des cartels de la drogue, ainsi que la menace qu'ils représentent pour la stabilité des États régionaux, sont à l'image des mesures de répression prises en 2022. L'accent a clairement été mis sur ceux qui « facilitent » l'activité des cartels. Ainsi, en juillet 2022, l'OFAC a sanctionné un individu qui, selon ce même Bureau américain, se livrait à un trafic d'armes d'envergure à destination du CJNG, l'un des principaux cartels du Mexique. En octobre, un avocat qui blanchissait de l'argent de la drogue pour le compte du cartel de Sinaloa a été condamné à une peine de plus de 15 ans à purger dans une prison américaine.

L'accélération de la production de cocaïne s'est heurtée au défi de taille et croissant que pose de la consommation de drogues de synthèse et opiacées aux États-Unis et au Canada

en particulier. En novembre 2022, le Groupe d'action financière (GAFI) a publié son premier rapport sur le blanchiment d'argent provenant du fentanyl et des opioïdes synthétiques. Comme au moins 82 % des overdoses liées aux opioïdes impliquent des opioïdes synthétiques, l'administration Biden a indiqué son intention de déployer une réponse « pangouvernementale. »

Ces pressions ne feront que s'intensifier à mesure que la pandémie reculera et que la vie nocturne lucrative reprendra ses droits à travers le monde. En 2022, les autorités de régulation et les forces de l'ordre de pays comme les États-Unis et l'Australie se sont concentrées sur les risques de blanchiment d'argent associés aux entreprises à forte circulation d'espèces. Le Centre australien de déclaration et d'analyse des transactions (AUSTRAC) a lancé une campagne nationale d'information à destination des pubs et des clubs et a rendu visite à plus de 200 établissements. L'AUSTRAC a également lancé des mesures d'exécution à l'encontre de plusieurs établissements.

Quelles conséquences pour mon entreprise ?

« Les établissements doivent apprécier et comprendre pleinement leur exposition, non seulement au trafic de drogue lui-même, mais aussi aux typologies associées qui pourraient révéler des activités liées aux stupéfiants. Le rapport du GAFI met en lumière des comportements tels que le blanchiment d'argent par le biais d'entreprises qui brassent beaucoup d'espèces ainsi que le blanchiment via le commerce et les virements électroniques, notamment entre sociétés fictives et sociétés écrans. Ce document explique aussi qu'il est essentiel d'améliorer le partage de l'information, la formation des enquêteurs ainsi que la sensibilisation aux risques liés aux nouvelles technologies que sont les places de marché sur le Dark Web. Les entreprises de services financiers destinés au grand public doivent garder à l'esprit que l'augmentation du trafic a des répercussions sur la vie de tous les jours. En effet, le trafic finit par se traduire par une criminalité de rue, dont les mules financières font partie, ou par des activités « régionalisées » comme observées au Royaume-Uni, y compris au sein de juridictions fort éloignées des pays d'où proviennent les drogues illégales. »

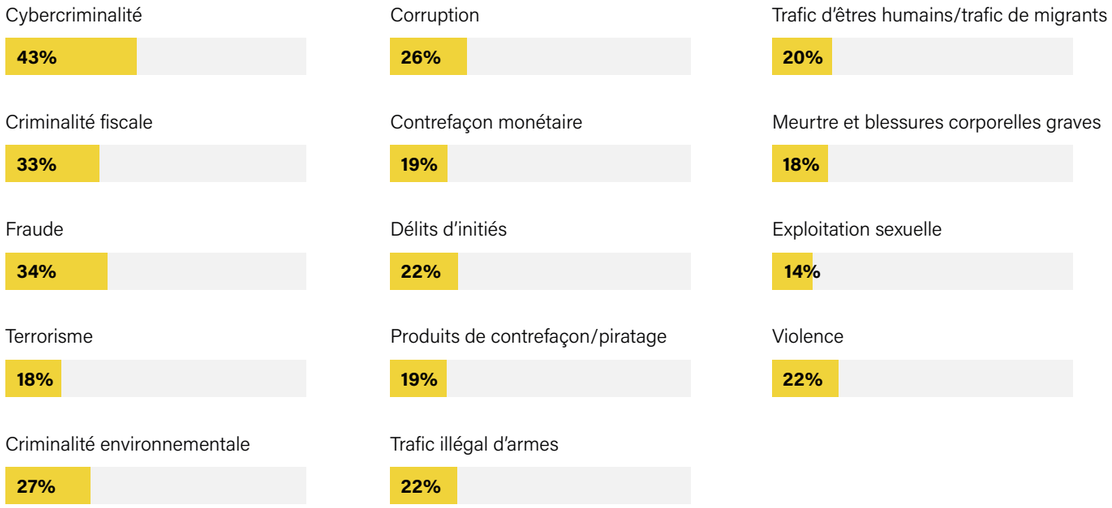
Iain Armstrong
spécialiste des affaires réglementaires chez ComplyAdvantage

La criminalité environnementale augmente car la répression faillit

Les préoccupations internationales concernant les crimes contre l'environnement et le trafic d'espèces sauvages sont allées crescendo en 2022, tout comme les menaces qui pèsent sur la sécurité alimentaire et la stabilité politique ainsi que les conflits et les migrations forcées. Interrogés sur les infractions majeures les plus importantes pour eux, plus d'un établissement sur quatre mentionnent les crimes environnementaux, ce qui en fait l'une des principales infractions dénoncées. Et ce alors que ce type de criminalité figure dans notre enquête pour la première fois en 2022. De même, la criminalité environnementale est la deuxième typologie la plus préoccupante pour les établissements qui soumettent des rapports d'activités suspectes (SAR), juste derrière l'évasion fiscale.

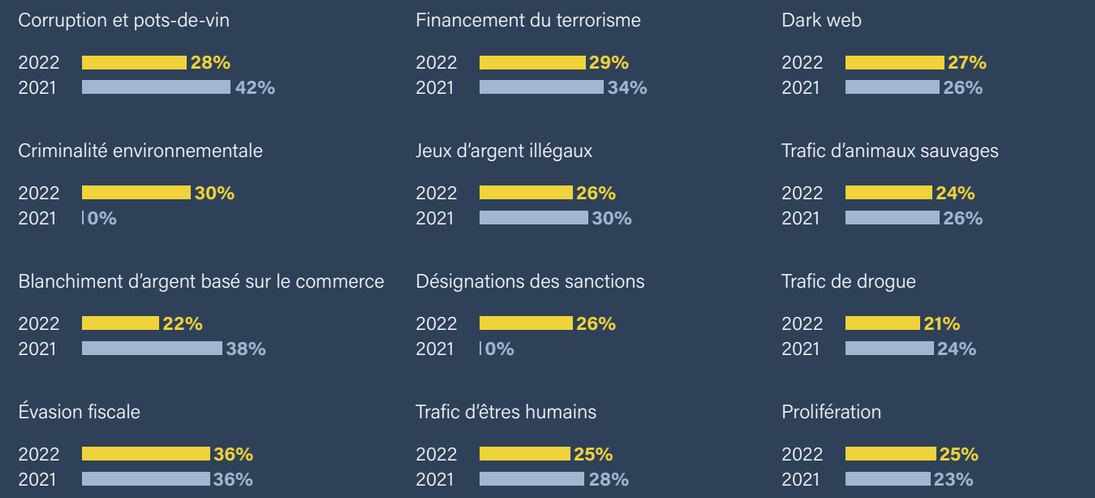
La situation mondiale se reflète dans les préoccupations des responsables de la conformité. Le groupe de réflexion Chatham House a constaté que 15 % de l'ensemble des exportations de bois de 37 pays exportateurs étaient illégales, la majorité provenant de Chine, du Brésil, d'Indonésie et de Russie. Les crimes contre la faune et la flore ont également augmenté avec l'Afrique du Sud qui connaît des niveaux records de braconnage pour répondre à la forte demande de l'Asie. En octobre 2022, l'opération d'un mois menée par l'Organisation mondiale des douanes (OMD) et destinée à faire respecter le cadre réglementaire de la CITES et à enrayer la criminalité liée aux espèces sauvages a concerné 125 pays. Elle a permis d'identifier 141 entreprises soupçonnées de se livrer à des ventes illégales, en plus de 2200 saisies et de l'ouverture de nombreuses enquêtes.

Quelles sont les infractions principales les plus importantes pour votre organisation ?



Source : ComplyAdvantage, L'état de la criminalité financière en 2023

Lorsque vous soumettez des rapports d'activités suspectes, quelle(s) typologie(s) préoccupe(nt) le plus votre entreprise ?



Source : ComplyAdvantage, L'état de la criminalité financière en 2023

Un nombre croissant de canaux en ligne, parmi lesquels les sites de commerce électronique, les médias sociaux et le commerce extraterritorial, sont également utilisés pour alimenter les cybercrimes contre la vie sauvage et vendre des marchandises en dehors du **cadre réglementaire de la CITES**. Ainsi, une enquête menée par le WWF, organisation de protection de la nature de premier plan, a révélé que le commerce illégal d'espèces sauvages en ligne au Myanmar a augmenté de **74 % entre 2020 et 2021**. Les réseaux privés virtuels (VPN), les serveurs proxy, le routeur TOR, le Darknet, les fournisseurs de paiements mobiles, les cryptomonnaies, les vidéos TikTok et les applications chiffrées de bout en bout sont utilisés pour vendre des biens illicites et garantir l'anonymat des criminels. Quant à la Coalition pour mettre fin au trafic d'espèces sauvages en ligne, elle a constaté que des fournisseurs Internet ont **bloqué ou supprimé plus de 11,6 millions de publications** et catalogues d'espèces sauvages mises en vente illégalement. En outre, cette coalition a reçu par le biais de son programme scientifique citoyen Cyber Spotter des rapports indiquant l'existence de plus de 11 000 annonces illégales concernant des espèces sauvages. Cette tendance est susceptible de se poursuivre.

La croissance de la demande, qui est à l'origine des crimes contre l'environnement et la faune sauvage, peut s'expliquer en partie par l'assouplissement des restrictions liées à la pandémie de Covid, ce qui a redynamisé des activités telles que le braconnage. En juin 2022, la Chine a **également suspendu l'interdiction du commerce d'espèces sauvages** décrétée en janvier 2020 pour s'attaquer aux sources potentielles de propagation du Covid. Le ralentissement de l'économie mondiale a déjà eu pour conséquence une **réduction des ressources** qui a entraîné une diminution des capacités de formation des gardes forestiers et des enquêteurs dans des pays comme le Botswana, l'Afrique du Sud, le Kenya, la Namibie et la Tanzanie. Dans ce contexte, **United for Wildlife** estime que le trafic d'espèces sauvages illégales « sera à nouveau pleinement profitable d'ici 2 à 3 ans. »

Les décideurs politiques et les autorités de régulation du monde entier en ont pris bonne note. Ainsi, en novembre 2022, la Commission européenne a adopté un nouveau **plan d'action européen** pour mettre fin au commerce illégal d'espèces sauvages. Les objectifs de ce plan sont notamment de s'attaquer aux causes racines du trafic d'espèces sauvages, de renforcer les cadres juridiques, d'appliquer plus efficacement la réglementation et d'améliorer les partenariats. Le parlement de Singapour a également abordé la question en avril 2022, le gouvernement soulignant le **« professionnalisme accru »** des criminels et l'importance croissante d'une « collaboration étroite entre le gouvernement et le secteur privé. » Aux États-Unis, en octobre 2022, l'**OFAC a sanctionné plusieurs ressortissants malaisiens** ainsi que la société Sunrise Greenland Sdn. Bhd. pour le « trafic cruel d'espèces sauvages menacées et en voie de disparition et de produits issus d'un braconnage brutal. » Cela concernait notamment le transport de cornes de rhinocéros, d'ivoire et de pangolins entre l'Afrique et le Vietnam et la Chine en passant par la Malaisie et le Laos.

Quelles conséquences pour mon entreprise ?

« Les établissements doivent mettre en place des contrôles anti-blanchiment permettant d'identifier et d'atténuer les risques de crimes environnementaux. Ils doivent aussi évaluer leur exposition au risque résiduel en lançant régulièrement des évaluations des risques à travers toute l'entreprise. En raison de l'émergence de nouvelles typologies de criminalité financière en lien avec l'environnement, les établissements financiers doivent fournir une formation adaptée et qui intègre des indicateurs et des typologies de risque pour les crimes liés à la faune sauvage illégale, au trafic de déchets et à d'autres crimes contre l'environnement. Les établissements doivent déployer des contrôles suffisamment pointus pour identifier et atténuer ces risques. Pour ce faire, ils doivent notamment améliorer leurs scénarios et règles de supervision des transactions afin de repérer les transactions et les comportements suspects et identifier ainsi des clients malveillants et des méthodes de paiement utilisées pour perpétrer des crimes environnementaux.

En outre, nous anticipons qu'en 2023 davantage d'établissements seront sensibilisés aux liens entre les crimes environnementaux et d'autres types de criminalité financière. Ainsi, les enquêtes menées avec succès concernant les crimes contre la faune et la flore sauvages révèlent systématiquement que ces crimes ont été facilités par des pots-de-vin et de la corruption de fonctionnaires ou de responsables portuaires, par le biais de fraude aux documents des douanes et aux accises et via du blanchiment d'argent avec dispersion des profits. Une prise de conscience accrue de cette intersectionnalité permettra aux établissements financiers de mieux comprendre, hiérarchiser et contrôler les risques de criminalité environnementale. »

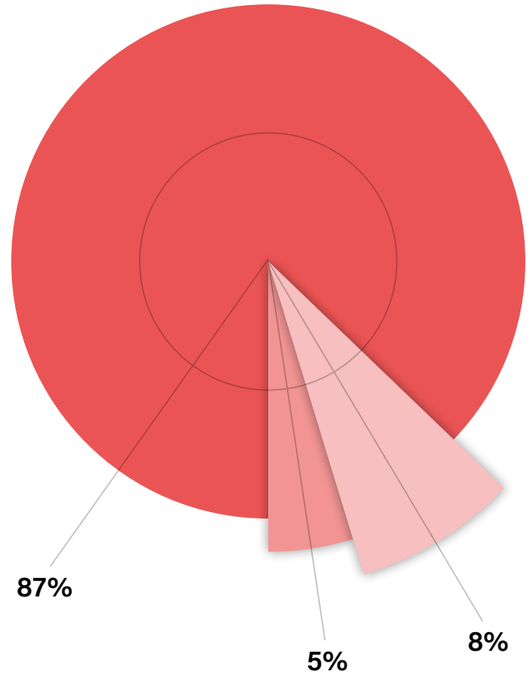
Alia Mahmud
spécialiste des affaires réglementaires chez ComplyAdvantage

Le crowdfunding, carburant de l'extrémisme politique

Les manifestations à Ottawa et aux postes-frontières entre les États-Unis et le Canada ont suscité une inquiétude internationale quant à l'utilisation des plateformes de financement participatif (crowdfunding) par des groupements extrémistes. Le 04 février 2022, GoFundMe a mis un terme à une campagne de soutien au « convoi de la liberté », craignant qu'il ne s'agisse d'une « occupation » et en raison de nombreux faits de violence. Le groupe à l'origine de cette mobilisation s'est alors tourné vers GiveSendGo, une plateforme qui, selon le Washington Post, s'affiche comme « leader de la collecte de fonds chrétienne » et via laquelle il a récolté plus de 9 millions de dollars.

Notre enquête internationale a posé pour la première fois cette année la question de l'utilisation de plateformes de financement décentralisées pour soutenir des groupements politiques extrémistes. 87% des personnes interogées dans le monde (82% en France) ont déclaré avoir noté une augmentation de l'utilisation de ces plateformes pour financer l'extrémisme. Le crowdfunding a également permis de soutenir des membres opérationnels de l'État islamique (EI) en Syrie. En effet, des rapports indiquent que des proches de jeunes hommes piégés dans des camps syriens ont tenté d'utiliser le service de messagerie Telegram pour « les mettre en sécurité ». Il est probable que certains de ceux qui cherchent à s'échapper ont l'intention de rejoindre les rangs de l'État islamique. Dans un rapport publié le 1er mars 2022, le département du Trésor américain a expliqué comment des groupements extrémistes nationaux ont utilisé des méthodes de collecte de fonds légales pour soutenir leurs activités, ce qui rend leur détection plus difficile. Le Trésor a également souligné le rôle de la pandémie qui a fait de ces plateformes « une nécessité plutôt qu'une solution commode. » En France, l'ordonnance du 30 mai 2014 a renforcé le rôle des plateformes de financement participatif.

Au cours des 12 derniers mois, quel changement avez-vous constaté dans l'utilisation des plateformes financières décentralisées (par exemple, le crowdfunding) pour financer des groupes groupes politiques extrémistes ?



Source : ComplyAdvantage, L'état de la criminalité financière en 2023

Quelles conséquences pour mon entreprise ?

« Il est manifeste que de nombreuses plateformes de crowdfunding ont été prises de court par l'engouement pour leurs offres de services. Associé aux cryptomonnaies et aux médias sociaux, le financement participatif augmente les risques de financement du terrorisme en permettant à des acteurs malveillants d'utiliser l'influence des plateformes de crowdfunding et les technologies liées aux cryptomonnaies pour obtenir le soutien de partisans et collecter des fonds. Les responsables Conformité d'établissements proposant des services financiers décentralisés doivent maîtriser la réglementation émergente concernant l'espace des cryptomonnaies et du crowdfunding pour déployer des solutions de contrôle de la criminalité financière à la fois pertinentes, efficaces et évolutives. Cela nécessitera aussi d'adapter les règles de supervision des transactions aux typologies et aux comportements uniques que les établissements doivent identifier. Les fournisseurs de plateformes de financement participatif doivent quant à eux se familiariser avec la nouvelle réglementation européenne relative aux prestataires de services de crowdfunding. Les banques et autres fournisseurs travaillant avec des entreprises de financement participatif doivent se soumettre à une obligation de vigilance accrue avant d'accepter un partenariat, sous peine de s'exposer aux risques de criminalité financière et de mauvaise publicité qui en découlent. »

Alia Mahmud
spécialiste des affaires réglementaires
chez ComplyAdvantage

A propos de ComplyAdvantage

ComplyAdvantage est la principale source de technologie de détection et de données sur le risque de criminalité financière fondée sur l'IA dans l'industrie financière. ComplyAdvantage a pour mission de neutraliser le risque de blanchiment d'argent, de financement du terrorisme, de corruption, ainsi que tous les autres crimes à caractère financier. Plus de 1000 entreprises dans 75 pays comptent sur ComplyAdvantage pour comprendre le risque lié aux entités avec lesquelles elles font affaire, grâce à la seule base de données globale et en temps réel au monde de personnes et de sociétés. La société identifie quotidiennement des dizaines de milliers d'événements à risque à partir de millions de points de données structurés et non structurés. ComplyAdvantage possède quatre plateformes mondiales implantées à New York, Londres, Singapour et Cluj-Napoca. La société est soutenue par Goldman Sachs, Ontario Teachers', Index Ventures et Balderton Capital.

Nos clients

Santander · Allianz · Lydia · qonto · raisin. · luko · SPENDESK · MANGOPAY

Contact

EMEA
France

Demandez une présentation

COMPLY ADVANTAGE®